ENTERASYS

Element Manager 2.2.1

MultiSwitch 700
User's Guide

Notice

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Virus Disclaimer

Enterasys has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Enterasys Networks makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © 2000 by Enterasys Networks. All rights reserved.

Printed in the United States of America.

Order Number: 9032895-02 April 2000

Enterasys Networks
P.O. Box 5005
Rochester, NH 03866-5005

Enterasys, NetSight, and **Matrix E7** are trademarks of Enterasys Networks.

SPECTRUM, **MiniMMAC**, **FNB**, **Multi Media Access Center**, and **DNI** are registered trademarks, and **Portable Management Application**, **IRM**, **IRM2**, **IRM3**, **IRBM**, **ETSMIM**, **EFDMIM**, **EMME**, **ETWMIM**, **FDMMIM**, **FDCMIM**, **MRXI**, **MRXI-24**, **NB20E**, **NB25E**, **NB30**, **NB35E**, **SEHI**, **TRBMIM**, **TRMM**, **TRMMIM**, **TRXI**, **Media Interface Module**, **MIM**, and **Flexible Network Bus** are trademarks of Cabletron Systems, Inc.

UNIX and **OPENLOOK** is a trademark of Unix System Laboratories, Inc. **OSF/Motif** and **Motif** are trademarks of the Open Software Foundation, Inc. **X Window System** is a trademark of Massachusetts Institute of Technology. **Ethernet** and **XNS** are trademarks of Xerox Corporation. **Apple** and **AppleTalk** are registered trademarks of Apple Computer, Inc. **Banyan** is a registered trademark of Banyan Systems, Inc. **DECnet** is a registered trademark of Digital Equipment Corporation. **Novell** is a registered trademark of Novell, Inc. **CompuServe** is a registered trademark of CompuServe. **Sun Microsystems** is a registered trademark, and **Sun**, **SunNet**, and **OpenWindows** are trademarks of Sun Microsystems, Inc.

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

   Enterasys Networks, 35 Industrial Way, Rochester, New Hampshire 03867.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.

   (b) This computer software may be:

   (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;

   (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;

   (3) Reproduced for safekeeping (archives) or backup purposes;

   (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;

   (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and

   (6) Used or copied for use in or transferred to a replacement computer.

   (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

   (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.

   (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

Contents

Chapter 1 Introduction

Chapter 2 The MultiSwitch 700 Device View

Chapter 3 Statistics

Chapter 4 Alarm Configuration

Chapter 5 FDDI Management

Chapter 6 ATM Configuration

Chapter 7 WAN Configuration

Index

Chapter 1

Introduction

About the MultiSwitch 700; how to use this guide; related guides; software conventions; getting help

Welcome to the ***MultiSwitch 700 Modules User's Guide***. We have designed this guide to serve as a reference for using NetSight Element Manager for the MultiSwitch 700 product, which encompasses the DLM6C-AA chassis and the MultiSwitch 700 modules.

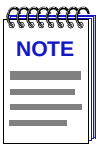
The MultiSwitch 700 product encompasses the DLM6C-AA chassis and the MultiSwitch 700 modules. The DLM6C-AA hub is a stand-alone chassis that offers five slots for interface modules; it also has two slots for dual redundant power supplies (installed vertically to the right of the module slots), and a removable fan tray (installed horizontally across the bottom the chassis).

At the heart of the MultiSwitch 700 is its Frame Transfer Matrix (FTM) backplane and distributed processing power. The FTM's passive design provides a separate independent backplane connection from each module in the chassis to every other module installed in the chassis; each module contains its own active switching components (so switching horsepower increases with module density), and each module can be managed independently (via its Module Manager management component) or — for devices which support distributed management — as part of the chassis unit (via a single chassis IP / MAC address pair and the Chassis Manager management component).

There are several varieties of MultiSwitch 700 modules currently available:

- The **DLE22-MA** and **DLE23-MA** modules each provide 24 fixed 10Base-T switch ports (via RJ45 connectors on the DLE22-MA; RJ21 Telco connectors on the DLE23-MA) and two slots for optional Fast Ethernet port interface modules. Several Fast Ethernet port interface modules are available:
  - the **DELFX-UI**, which provides one multi-mode fiber port via an SC connector;
  - the **DELTX-UI**, with one Category 5 UTP RJ45 connector;
  - and the **DELF3-UI**, with one single-mode fiber port via an SC connector.

- The **DLE32-MA** and **DLE33-MA** modules each provide 24 fixed 10Base-T switch ports (via RJ45 for the DLE32-MA and RJ21 for the DLE33-MA) and one slot for an optional modular interface that can link the chassis to an FDDI, ATM, WAN, or Gigabit Ethernet backbone. Each modular interface provides frame translation between ATM, FDDI, WAN, Gigabit Ethernet, and Ethernet through an on-board Intel i960 processor:
  - The **DELHF-UA** is an FDDI / Ethernet Translator, which can act as a Single Attached Station (SAS) or Dual Attached Station (DAS) on an external FDDI ring. FDDI Port Interface Modules provide a wide range of media connectivity to the ring. The DELHF-UA also has full-duplex capability, allowing for a 200 Mbps connection to another DELHF-UA.
  - The **DELHA-UA** is an Asynchronous Transfer Mode (ATM) modular interface, which provides an ATM uplink via two media-configurable ATM Port Interface Modules. The dual port interface module design allows for a redundant connection to the uplink, so that if the primary interface fails, the secondary interface will automatically take over. The DELHA-UA acts as an ATM Forum LAN Emulation Client (LEC) so that it can transfer data between devices on an 802.x LAN supported by the MultiSwitch 700 and ATM-connected end stations across a high speed ATM Link. The DELHA-UA adheres to the ATM Forum-approved LAN Emulation (LANE) standard, which defines how end users that rely on existing data communications technology and protocols can operate over an ATM network without penalty.
  - The **DELHW-UA** is a Wide Area Networking (WAN) modular interface, which can provide uplinks to WAN backbones and allow you to perform seamless LAN to WAN switching. The **DELHW-UA** supports IP and IPX bridging or routing services, including IP RIP. Multiple WAN connectivity options are supported, including Sync, T1, E1, D&I, ISDN S / T, DDS, and HDSL interfaces, through the use of two configurable WAN port interface modules. Connectivity is available for Point to Point Protocol (PPP), as well as Frame Relay and Leased Lines. Each WAN port interface module can act independently, allowing simultaneous communication, or configured to provide redundant channels if desired.



Unlike other modular interfaces designed for the MultiSwitch 700 boards, the DELHW-UA module functions as an independent intelligent device with its own IP address. As such, it must be managed separately from the MultiSwitch 700 chassis and the board on which it is installed.

The DELHW-UA's WAN functionality is accessed from the DELHW-UA's Device View. See ***The DELHW-UA Device View****, on page 2-75 of Chapter 2,* ***The MultiSwitch 700 Device View****, for instructions on launching the DELHW-UA Device View. Other DELHW-UA Device View functions, such as finding a source address and changing the device time and date, are also described there.*

Chapter 7, ***WAN Configuration****, provides information on configuring and managing the WAN capabilities of the various port modules available for the DELHW-UA.*

  - The **DELHG-UA** and **DELHL-UA** are Gigabit Ethernet modular interfaces, each of which provide a single Gigabit Ethernet connection that fully conforms to the IEEE P802.3z (D3.1) Draft Standard. The **DELHG-UA** provides a single 1000Base-SX (short-wave) multimode fiber optic SC interface, allowing for link distances of up to 500 meters. The **DELHL-UA** provides a single 1000Base-LX (long-wave) single mode / multimode fiber optic SC interface, allowing for link distances of up to 3 kilometers.

- The **DLE28-MA** module provides 24 fixed Ethernet multi-mode fiber ports via ST connectors, plus a single slot for a modular interface.
- The **DLE49-MA** module provides 48 switched Ethernet ports via four RJ21 Telco connectors and a single modular interface slot.
- The **DLE02-MA** and **DLE52-MA** modules are 10 / 100 Fast Ethernet modules. The DLE02-MA provides 24 ports via RJ45 connections. The DLE52-MA provides 16 ports via RJ45 connections as well as a next-generation modular interface slot, which can accept any of the previously detailed modular interfaces, or the new **DELVM-UA** Gigabit Ethernet modular interface:
  - The **DELVM-UA** is a Gigabit Ethernet module which provides two slots for Gigabit Ethernet port interface modules of various media to offer integrated Gigabit Ethernet uplink capability. The DELVM-UA can accept the **DELG1-UA**, which offers one SC connector for MMF 1000Base SX Gigabit Ethernet connectivity, the **DELG9-UA**, which offers one SC connector for MMF or SMF 1000Base LX connectivity, or the **DELG4-UA**, which offers one ANSI Fibrechannel style-2 connector for 150 Ohm STP 1000Base CX connectivity.
- The **DLEHF-MA** carrier module provides two Fast Ethernet port interface module slots and two modular interface slots.

Each of these modules provide key mission-critical features such as redundant links for load sharing, alarm thresholding, broadcast storm control, port redirecting for traffic analysis, traffic priority configuration, and full error breakdown. Per-port RMON support is also provided. By default, these modules perform traditional switching (or bridging); each can also be configured to perform prestandard IEEE 802.1Q VLAN switching (a.k.a “port-based VLAN” switching).

The DLM6C-AA MultiSwitch 700 chassis itself offers the following features:

- Slots for up to 5 double-wide 2.4" interface modules, with chassis-wide support of up to 130 users. Each interface module is individually driven and managed by on-board processors, including an onboard ASIC processor for switching, and Intel i960 Host microprocessors for dedicated module management.
- A Frame Transfer Matrix (FTM) backplane design, that provides a separate independent backplane connection from each module in the chassis to every other module installed in the chassis. This allows a backplane bandwidth capacity of up to 3.2 Gbps.

- Support for redundant, load-sharing power supplies to provide fault tolerance.
- Diagnostic LEDs for quick visual diagnosis of interface and device performance; a single removable fan tray; a 19" footprint for ease of installation in rack mounts; and front panel accessibility to all chassis components for easy maintenance.
- A distributed chassis management design, in which each module in the chassis can be managed via a single chassis IP / MAC address pair that is associated with the chassis as a whole. Each installed module will respond to management queries to the “Chassis Manager” component that use the chassis IP / MAC address pair and a chassis-level community string (e.g., “public”).

  In addition to the “Chassis Manager” component for the hub as a whole, each installed module supports its own “Module Manager” management component that responds to the same chassis IP / MAC pair and a uniquely indexed module-level community string (e.g., “public.1” for module 1; “public.2” for module 2, etc.).

Using the MultiSwitch 700 Modules User’s Guide

Each chapter in this guide describes one major functionality or a collection of several smaller functionalities of the MultiSwitch 700 modules and the chassis in which they are installed. This guide contains information about software functions which are accessed directly from the device icon.

Because the modules share much of their functionality, they will be collectively referred to as the MultiSwitch 700 modules. Where there are differences, however, each device will be named separately, as necessary. The information displayed in many of the windows will differ slightly depending upon which type of device is being managed; however, only a single window will be shown unless significant differences in functionality exist.

Chapter 1, **Introduction**, provides a list of related documentation, describes certain software conventions, and shows you how to contact the Global Technical Assistance Center. It also briefly describes the MultiSwitch 700 modules and chassis.

Chapter 2, **The MultiSwitch 700 Device View**, describes the visual display of the MultiSwitch 700 chassis as a whole and explains how to use the mouse within the Device View. It details all chassis-level management functions, including Port Redirect, Advanced Priority Configuration, and pre-standard 802.1Q port-based VLAN configuration at the chassis level. It documents chassis-specific information, including MIB-II System Group information, chassis IP and MAC addresses, chassis clock information and uptime, power supply configuration and status, fan operational status, and backplane configuration.

The chapter also details how each module is displayed in the chassis, and explains how to access management menus from the module display and change port status information. It explains how to manage the individual module by

monitoring the module's system resources, finding a source address on the module, establishing module-level port priorities, setting up broadcast suppression on the device, and configuring the module's front panel COM port and any attached Uninterruptable Power Supply (UPS).

Also described in this chapter is the Device View functionality associated with the DELHW-UA modular interface. Unlike other modular interfaces designed for the MultiSwitch 700 boards, the DELHW-UA module functions as an independent intelligent device with its own IP address. As such, it must be managed separately from the MultiSwitch 700 chassis and the board on which it is installed.

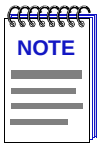
Chapter 3, **Statistics**, describes the two statistics views available at the interface level: MIB-II Interface statistics and RMON Ethernet statistics.

Chapter 4, **Alarm Configuration**, provides instructions for using both the Basic and Advanced alarm applications to configure alarms and the events that notify you that an alarm condition has occurred. The ability to automatically initiate a SET or a series of SETs in response to an alarm — functionality provided by the proprietary Actions MIB — is also described.

Chapter 5, **FDDI Management**, describes the Configuration, Connection Policy, Station List, Performance, FDDI Statistics, and Frame Translation selections available when a DELHF-UA module is installed.

Chapter 6, **ATM Configuration**, discusses the ATM Connections window which will appear if you have a DELHA-UA module installed in your device.

Chapter 7, **WAN Configuration**, describes the physical configuration of the DELHW-UA modular interface, including port interface module options, and explains the WAN Logical View window and its functions.



The **SmartSwitch and MultiSwitch Chassis User's Guide** *discusses how to configure the MultiSwitch 700 chassis using the Chassis Setup view. It gives an overview of MultiSwitch 700 management views and general module information, and discusses changing the current view as well as the default view.*

Related Manuals

The **MultiSwitch 700 Modules User's Guide** is only part of a complete document set designed to provide comprehensive information about the features available to you through NetSight Element Manager. Other guides which include important information related to managing the MultiSwitch 700 include:

SmartSwitch and MultiSwitch Chassis User's Guide

User's Guide

Tools Guide

Remote Administration Tools User's Guide

Remote Monitoring (RMON) User's Guide

Alarm and Event Handling User's Guide

For more information about the capabilities of the MultiSwitch 700, consult the appropriate hardware documentation.

Software Conventions

NetSight Element Manager's device user interface contains a number of elements which are common to most windows and which operate the same regardless of which window they appear in. A brief description of some of the most common elements appears below; note that the information provided here is not repeated in the descriptions of specific windows and / or functions.

Common Window Fields

Similar descriptive information is displayed in boxes at the top of most device-specific windows in NetSight Element Manager, as illustrated in Figure 1-1.

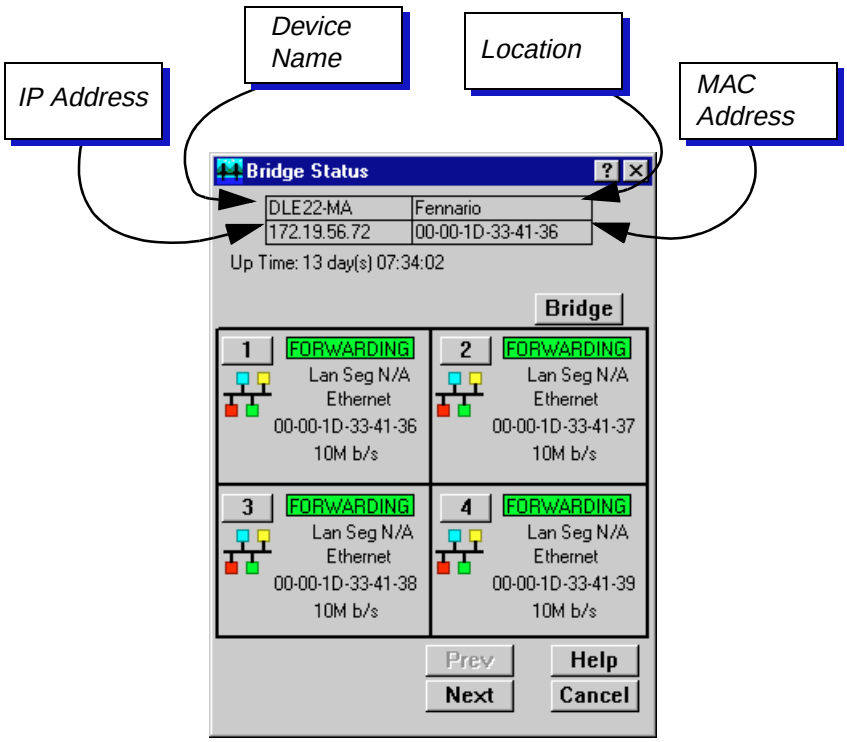


Figure 1-1. Sample Window Showing Group Boxes

Device Name

Displays the user-defined name of the device. The device name can be changed via the System Group window; see the ***Generic SNMP User's Guide*** for details.

IP Address

Displays the device's IP (Internet Protocol) Address. This will be one of two addresses:

- The Network IP address assigned to the MultiSwitch 700 chassis (if a network-level IP address has been assigned to the module).
- The individual module IP address (if IP addresses have been assigned on a per-module basis).

Both of these IP address are assigned via Local Management to the Host interface of each module in the MultiSwitch 700 chassis. The IP addresses cannot be changed remotely via NetSight Element Manager. Note that although each interface on the MultiSwitch 700 module has its own MAC, or physical, address, only a single IP address is assigned to the module or chassis as a whole.

Location

Displays the user-defined location of the device or chassis. The location is entered through the System Group window; see the ***Generic SNMP User's Guide*** for details.

MAC Address

Displays the manufacturer-set MAC address associated with the network IP address of the MultiSwitch 700 chassis, or the module IP address of the currently monitored MultiSwitch 700 module. Note that MAC addresses are factory-set and cannot be altered through management.

Using the Mouse

This document assumes you are using a Windows-compatible mouse with two buttons; if you are using a three button mouse, you should ignore the operation of the middle button when following procedures in this document. Procedures within the NetSight Element Manager document set refer to these buttons as follows:

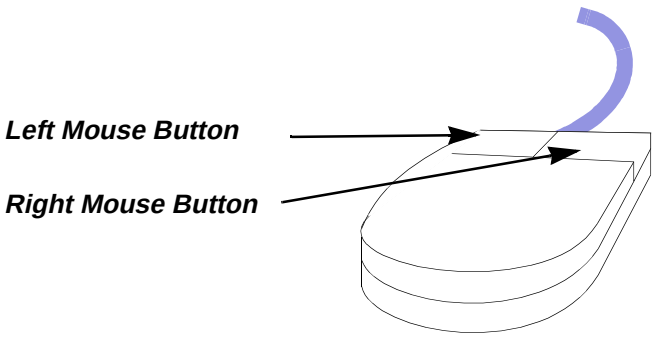


Figure 1-2. Mouse Buttons

For many mouse operations, this document assumes that the left (primary) mouse button is to be used, and references to activating a menu or button will not include instructions about which mouse button to use.

However, in instances in which right (secondary) mouse button functionality is available, instructions will explicitly refer to **right** mouse button usage. Also, in situations where you may be switching between mouse buttons in the same area or window, instructions may also explicitly refer to both **left** and **right** mouse buttons.

Instructions to perform a mouse operation include the following terms:

- **Pointing** means to position the mouse cursor over an area without pressing either mouse button.
- **Clicking** means to position the mouse pointer over the indicated target, then press and release the appropriate mouse button. This is most commonly used to select or activate objects, such as menus or buttons.
- **Double-clicking** means to position the mouse pointer over the indicated target, then press and release the mouse button two times in rapid succession. This is commonly used to activate an object's default operation, such as opening a window from an icon. Note that there is a distinction made between "click twice" and "double-click," since "click twice" implies a slower motion.
- **Pressing** means to position the mouse pointer over the indicated target, then press and hold the mouse button until the described action is completed. It is often a pre-cursor to Drag operations.
- **Dragging** means to move the mouse pointer across the screen while holding the mouse button down. It is often used for drag-and-drop operations to copy information from one window of the screen into another, and to highlight editable text.

Using Buttons

The **Cancel** button that appears at the bottom of most windows allows you to exit a window and terminate any unsaved changes you have made. You may also have to use this button to close a window after you have made any necessary changes and set them by clicking on an **OK**, **Set**, or **Apply** button.

An **OK**, **Set**, or **Apply** button appears in windows that have configurable values; it allows you to confirm and SET changes you have made to those values. In some windows, you may have to use this button to confirm each individual set; in other windows, you can set several values at once and confirm the sets with one click on the button.

The **Help** button brings up a Help text box with information specific to the current window. For more information concerning Help buttons, see **Getting Help**, on page 1-9.

The command buttons, for example **Bridge**, call up a menu listing the windows, screens, or commands available for that topic.

Any menu topic followed by ... (three dots) — for example **Statistics...** — calls up a window or screen associated with that topic.

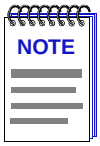
Getting Help

This section describes three different methods of getting help for questions or concerns you may have while using NetSight Element Manager.

Using On-line Help

You can use the **Help** buttons to obtain information specific to a particular window. When you click on a Help button, a window will appear which contains context-sensitive on-screen documentation that will assist you in the use of the windows and their associated command and menu options. Note that if a Help button is grayed out, on-line help has not yet been implemented for the associated window.

From the **Help** menu accessed from the Device View window menu bar, you can access on-line Help specific to the Device View window, as well as bring up the Chassis Manager window for reference. Refer to Chapter 2, **The MultiSwitch 700 Device View**, for information on the Device View and Chassis Manager windows.



All of the online help windows use the standard Microsoft Windows help facility. If you are unfamiliar with this feature of Windows, you can select ***Help*** *from the Windows* ***Start*** *menu, or* ***Help —>How to Use Help*** *from the primary NetSight Element Manager window.*

Accessing On-line Documentation

The complete suite of documents available for NetSight Element Manager can be accessed via a menu option available from the primary window menu bar: **Help —> Online Documents**. If you chose to install the documentation when you installed NetSight Element Manager, this option will launch Adobe's Acrobat Reader and a menu file, which provides links to all available documents.

*If you have not yet installed the documentation, the **Online Documents** option will not be able to access the menu file; in order to activate this option, you must run the **setup.exe** again to install the documentation component. See your* **Installation Guide** *for details.*

Getting Help from the Global Technical AssistanceCenter

If you need technical support related to NetSight Element Manager, contact the Global Technical Assistance Center via one of the following methods:

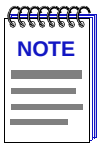
By phone:	(603) 332-9400 *24 hours a day, 365 days a year*
By fax:	(603) 337-3075
By mail:	Enterasys Networks Technical Support 35 Industrial Way Rochester, NH 03867
By e-mail mail:	support@enterasys.com
FTP:	ftp.ctron.com (134.141.197.25)
Login	`anonymous`
Password	`your e-mail address`
By BBS:	(603) 335-3358
Modem Setting	8N1: 8 data bits, 1 stop bit, No parity

Send your questions, comments, and suggestions regarding NetSight documentation to NetSight Technical Communications via the following address:

Netsight_docs@enterasys.com

To locate product specific information, refer to the Enterasys Web site at the following address:

http://www.enterasys.com



For the highest firmware versions successfully tested with NetSight Element Manager 2.2.1, refer to the ***Readme*** *file available from the NetSight Element Manager 2.2.1 program group. If you have an earlier version of firmware and experience problems running NetSight Element Manager, contact the Global Techncical Assistance Center for upgrade information.*

Chapter 2

The MultiSwitch 700 Device View

Information displayed in the Device View window; the logical Device View; the Chassis Manager window; hub management functions

The MultiSwitch 700 Device View window is the main screen that immediately informs you of the current configuration of your chassis via a graphical display of the chassis front panel. The default Logical View shows the modules installed in your chassis according to the physical slots they occupy, and displays the condition of individual interfaces on those modules. The Device View window serves as a single point of access to all other MultiSwitch 700 windows and screens, which are discussed at length in the following chapters.

To access the MultiSwitch 700 Device View window, use one of the following options:

Figure 2-1. MultiSwitch Device Icon

1. In any map, list, or tree view, double-click MultiSwitch 700 icon you wish to manage. The Management Selection window, Figure 2-2, opens.

   or

1. In any map, list, or tree view, click the device you wish to manage, and select **Manage—>Node** from the primary window menu bar, or select the Manage Node  toolbar button. The Management Selection window, Figure 2-2, opens.

   or

1. In any map, list, or tree view, click the **right** mouse button once to select the device you wish to manage.

2. Select **Manage** from the resulting menu. The Management Selection window, Figure 2-2, opens.

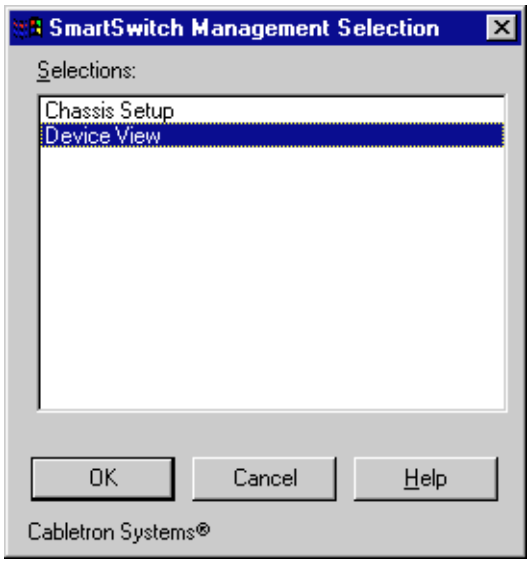


Figure 2-2. The Management Selection Window

3. In the Management Selection window, select **Device View**, and click the **OK** button. The MultiSwitch 700 Device View window, Figure 2-3, opens.

Viewing Device Information

The MultiSwitch 700 Device View window (Figure 2-3) provides a graphic representation of the MultiSwitch 700 hub and the currently modeled MultiSwitch 700 modules, including a color-coded port display which immediately informs you of the current configuration and status of all the port The module displays in its corresponding physical slot in the MultiSwitch 700. Slots are numbered from 1–5, from left to right in the chassis. The Device View also will provide you with environmental status information about the fan tray and power supplies installed in the chassis.

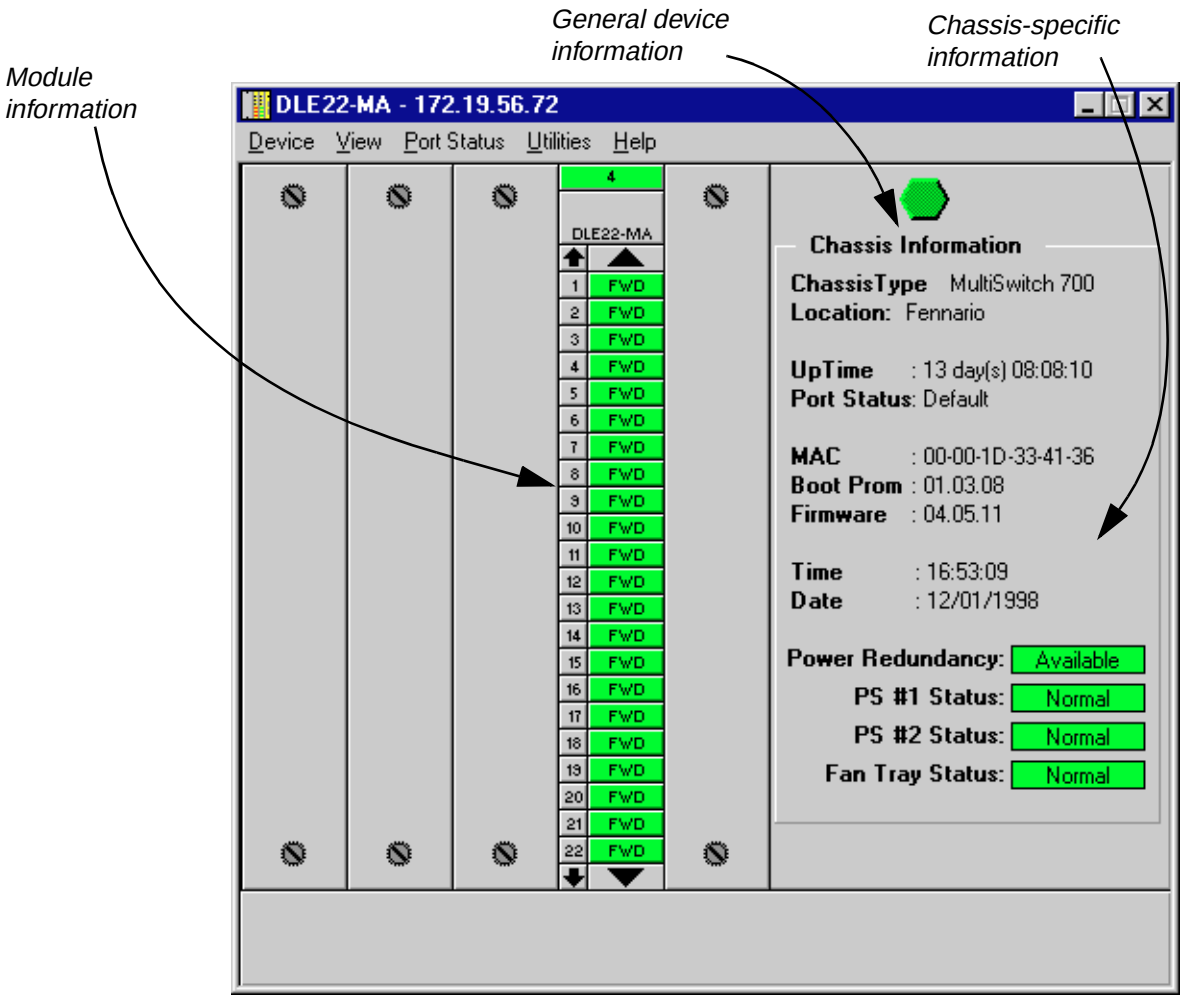
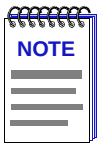


Figure 2-3. The MultiSwitch 700 Device View Window



Up to 22 ports can be displayed simultaneously on a module. If a module has a higher port density than 22 ports, arrows displays at the top and bottom of the port stack so that you can scroll through the remaining ports.

General Device Information

In addition to the main interface display, the Device View window provides the following device information:

IP

The Device View window title displays the device's IP (Internet Protocol) Address; this will be the MultiSwitch 700 module IP address used to define the device icon. The IP address is assigned to the MultiSwitch 700 module via the Device Configuration portion of Local Management; it cannot be changed via NetSight Element Manager. Note that although each interface in the MultiSwitch 700 module has its own MAC, or physical, address, only a single IP address is assigned to the device.

Connection Status 

This color-coded area indicates the current state of communication between NetSight Element Manager and the MultiSwitch 700 module.

- **Green** indicates the MultiSwitch 700 module is responding to device polls (valid connection).
- **Magenta** indicates that the MultiSwitch 700 module is in a temporary stand-by mode while it responds to a physical change in the hub (such as when a module is inserted). Note that module and port menus are inactive during this stand-by state.
- **Blue** indicates an unknown contact status; polling has not yet been established with the MultiSwitch 700 module.
- **Red** indicates the MultiSwitch 700 module is not responding to device polls (device is off line, or device polling has failed across the network for some other reason).

Chassis Type

The model of chassis — MultiSwitch 700—þin which the monitored MultiSwitch 700 module is installed.

Location

A descriptive field you can use to identify where the chassis is physically located. You can edit this field through the device's System Group window; refer to the ***Generic SNMP User's Guide*** for details.

UpTime

The amount of time, in a days hh / mm / ss format, that the MultiSwitch 700 module has been running since the last start-up. Note that when distributed chassis management is available, this field will indicate the time that the longest active module has been running since start-up.

Port Status

Indicates the port status display selection currently in effect. The default port status view is bridge status; if you have not changed the port status selection since launching the Device View window, this field will display **Default**. For more information about changing the port status display, see **Port Status Displays**, on page 2-12.

MAC

Displays the manufacturer-set MAC, or physical, address associated with the IP address used to define the device icon. This will be the MAC address assigned to the first interface detected on the MultiSwitch 700 module (although each interface in the MultiSwitch 700 module has its own MAC address). MAC addresses are factory-set and cannot be altered.

Boot Prom

The revision of BOOT PROM installed in the MultiSwitch 700 module.

Firmware

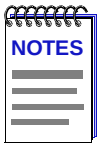
The revision of device firmware stored in the MultiSwitch 700 module's FLASH PROMs.

Time

The current time, in a 24-hour hh:mm:ss format, set in the MultiSwitch 700 module's internal clock.

Date

The current date, in an mm / dd / yyyy format, set in the MultiSwitch 700 module's internal clock.



NetSight Element Manager displays and allows you to set all dates with four-digit year values. You can set the date and time by using the ***Edit Device Date*** *and* ***Edit Device Time*** *options on the Device menu; see* ***Setting the Device Date and Time****, on page 2-72, for details.*

DLM6C-AA Chassis-specific Information

The Device View provides the following information about the DLM6C-AA chassis in which the MultiSwitch 700 module is installed. There are four color-coded fields which provide status information for the operation of the power supplies and fan tray installed in the DLM6C-AA chassis.

Power Redundancy

The DLM6C-AA supports two power supply modules. Each supports a separate AC input connector, so that two separate power sources can be used for the chassis. Additionally, with two power supplies installed, the total load presented by the DLM6C-AA and its installed modules is split 50/50 between the supplies (+/- 5%). The Power Redundancy field displays whether or not the chassis is currently configured for load sharing and power redundancy. Possible values are:

- Available (Green) — Two HA-205-XX power supply modules are installed in the DLM6C-AA chassis.
- Not Available (Yellow) — Only a single HA-205-XX power supply module is installed in the DLM6C-AA chassis. Note that when only a single power supply module is installed, it must always be in power slot 1 (PS1).

PS #1/#2 Status

Indicates the state of any power supplies installed in the DLM6C-AA Chassis. Possible states returned are:

- Not Available (Yellow) — No response has been returned from the device regarding the power supplies.
- Normal (Green) — A power supply is installed and operating in the associated power slot.
- Fault (Red) — The power supply in the associated power slot is not operational.
- Not Installed (Blue) — The indicated power slot is not occupied by a power supply.

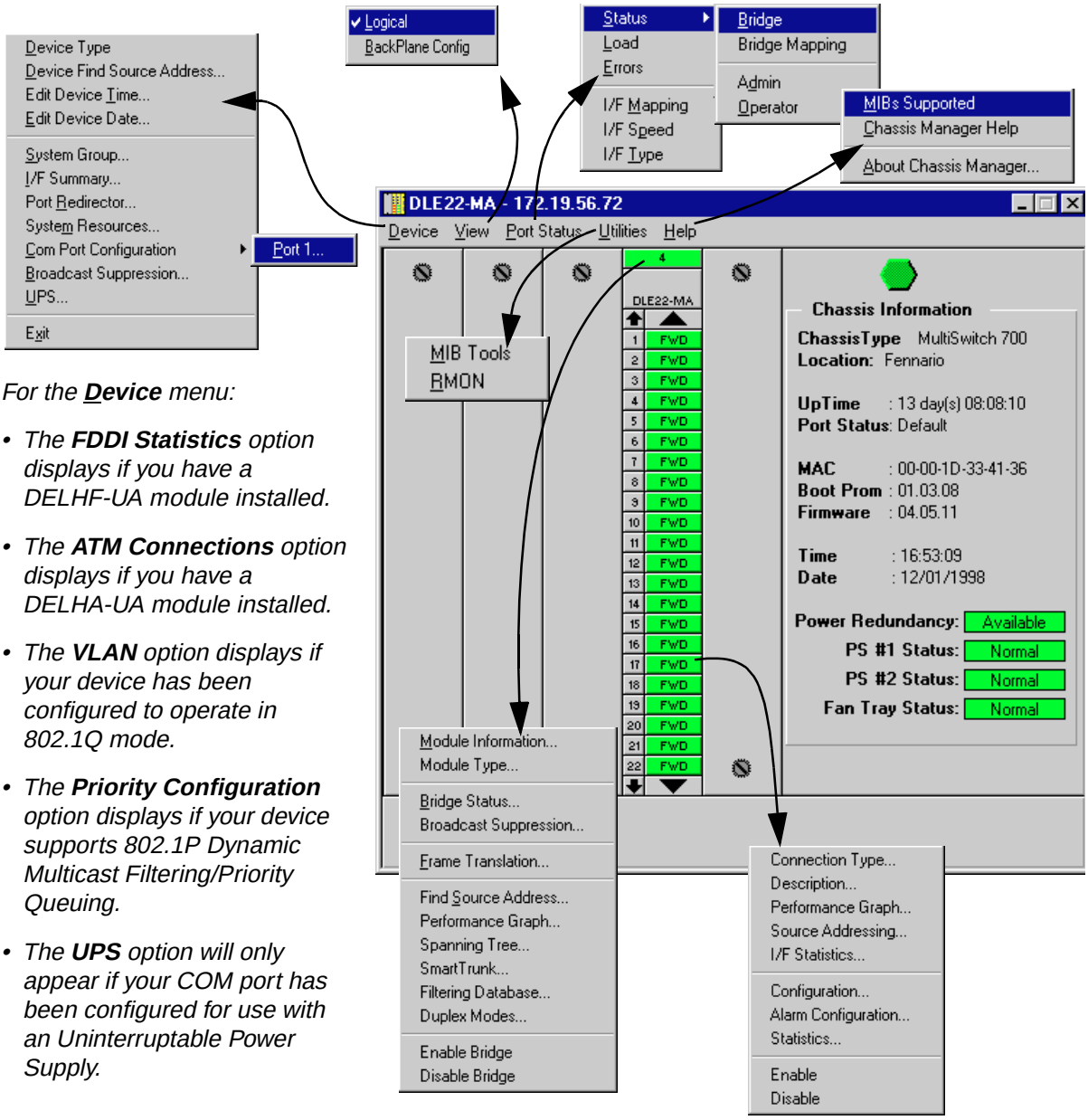
Fan Tray Status

The DLM6C-AA supports a single, removable fan tray that has four fans. The tray is hot swappable, so it can be removed without powering down the chassis. This field indicates the status of the DLM6C-AA's Fan Tray:

- Not Available (Yellow) — No response has been returned regarding the fan tray.
- Normal (Green) — A fan tray is installed and operational.
- Fault (Red) — One or more fans in the tray have failed.
- Not Installed (Blue) — The fan tray slot is not occupied. The chassis is in danger of overheating if it continues to run without the fan tray installed.

Menu Structure

By clicking on various areas of the MultiSwitch 700 Device View display, you can access menus with device-, module-, and port-level options, as well as utility applications which apply to the device. The following illustration displays the menu structure and indicates how to use the mouse to access the various menus:



*For the **Device** menu:*

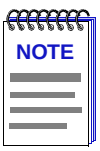
- *The **FDDI Statistics** option displays if you have a DELHF-UA module installed.*
- *The **ATM Connections** option displays if you have a DELHA-UA module installed.*
- *The **VLAN** option displays if your device has been configured to operate in 802.1Q mode.*
- *The **Priority Configuration** option displays if your device supports 802.1P Dynamic Multicast Filtering/Priority Queuing.*
- *The **UPS** option will only appear if your COM port has been configured for use with an Uninterruptable Power Supply.*

Figure 2-4. MultiSwitch 700 Device View Menu Structure

The Device Menu

From the Device Menu, you can access the following selections:

- **Device Type** displays a window containing a description of the device being modeled. See **Device Type**, on page 2-20, for details.
- **Device Find Source Address** enables you to determine through which interface a specified MAC address is communicating by searching the repeater Source Address Table (SAT) and the 802.1d bridge Filtering database. If the specified MAC address is located, a list of interface(s) through which the given address is communicating will be displayed. See **Using Device Find Source Address**, on page 2-27.
- **Edit Device Time** and **Edit Device Date** allow you to set the MultiSwitch 700 module's internal clock; see **Setting the Device Date and Time**, on page 2-72.
- **System Group** allows you to manage the MultiSwitch 700 via SNMP MIB II. Refer to the ***Generic SNMP Management Guide*** for further information.
- **I/F Summary** lets you view statistics (displayed both graphically and numerically) for the traffic processed by each network interface on your device. See **Viewing I/F Summary Information**, on page 2-22, for details.
- **VLAN** option displays in the Device menu if your module is configured to operate in 802.1Q mode. The windows launched via the **VLAN** option allow you to configure and operate port-based VLANs on the module. See **802.1Q VLANs**, on page 2-60, for details.
- **ATM Connections** option displays if you have a DELHA-UA installed in your module. This launches a window which lets you configure Permanent Virtual Circuits (PVCs) for the module. See Chapter 6, **ATM Configuration**, for more information.
- **Port Redirector** launches a window that allows you to mirror — or redirect — traffic received or transmitted at one port on your module to one or more other ports, so that you can unobtrusively attach network analyzers to ascertain problems or trends in your data flow. For more information about using the Port Redirector window, see **Redirecting Traffic on the MultiSwitch 700 Module**, on page 2-46.
- **System Resources** displays information about the processor used on the monitored MultiSwitch 700 module, as well as the amount of installed and currently available FLASH memory, DRAM, and NVRAM. See **The System Resources Window**, on page 2-57.
- **Priority Configuration** allows you to establish priority packet forwarding. For more information, see **Priority Configuration**, on page 2-48.



*The **Priority Configuration** menu option only displays for modules that respond to any of NetSight Element Manager's queries to the following OIDs: **ctPriorityExtPortStatus**, **ctPriorityExtMaxNumMACEntries**, or **ctPriorityExtNumPktTypeEntries**.*

- **Com Port Configuration** allows you to configure the settings of the COM ports on the MultiSwitch 700 module; see **Configuring the COM Port**, on page 2-29.
- **Broadcast Suppression** allows you to set a threshold on the number of broadcast packets issued from each port on the MultiSwitch 700 module when it is operating in traditional switch (bridge) mode. See **Broadcast Suppression**, on page 2-55.
- **FDDI Statistics** option displays if you have a DELHF-UA installed in your module. This launches a window which displays traffic-related statistics for each Station Management (SMT) entity present on an installed DELHF-UA. See Chapter 5, **FDDI Management**, for more information.
- **UPS** brings up a window that allows you to configure an Uninterruptable Power Supply attached to your MultiSwitch 700 Module's COM port. See **Using an Uninterruptable Power Supply (UPS)**, on page 2-43, for details.
- **Exit** closes the MultiSwitch 700 Device View window.

The View Menu

The View menu lets you switch the front panel display between two graphic representations of the device:

- The **Logical** view provides the logical front panel display of the MultiSwitch 700 module and its interfaces.
- The **BackPlane Config** view displays the backplane connections between the MultiSwitch 700 module and other modules installed in the DLM6C-AA chassis.

The Port Status Menu

The Port Status menu allows you to select the status information that will be displayed in the port text boxes in the Device View window:

- **Status** allows you to select one of four status type displays: Bridge, Bridge Mapping, Admin, or Operator.
- **Load** will display the portion of network load processed per polling interval by each interface, expressed as a percentage of its theoretical maximum load (10, 100, 155.5, 800, or 1000 Mbps).
- **Errors** allows you to display the number of errors detected per polling interval by each interface, expressed as a percentage of the total number of valid packets processed by the interface.
- **I/F Mapping** will display the interface *ifIndex* associated with each port on your MultiSwitch 700 module.
- **I/F Speed** will display the port's bandwidth: 10M (megabits) for Ethernet; 100M for Fast Ethernet; 1.00 G for Gigabit Ethernet; 155.5M for ATM; and 800M for the backplane interfaces.
- **I/F Type** will display the port type of each port on your MultiSwitch 700 module, e.g., Eth (ethernet-csmacd), ATM, or FDDI.

For more information on the port display options available via this menu, see **Selecting a Port Status View**, on page 2-12.

The FDDI Menu

If your MultiSwitch 700 has an installed DELHF-UA, the FDDI menu displays on the Device View menu bar, with the following options:

- **Configuration**
- **Connection Policy**
- **Station List**
- **Performance**
- **Frame Translation**

Refer to Chapter 5, **FDDI Management**, for information on these menu selections.

The Utilities Menu

The Utilities Menu provides the following options:

- MIB Tools, which provides direct access to the MultiSwitch 700 module's MIB information; refer to the ***Tools Guide*** for more information.
- RMON utility, a remote monitoring feature that is supported on a per-port basis when at least one Ethernet or Fast Ethernet module is installed in the chassis; refer to the ***RMON User's Guide*** for more information.

These selections are also available from the **Tools** menu at the top of the primary NetSight Element Manager window.

The Help Menu

The Help Menu has the following three selections:

- **MIBs Supported** brings up the Chassis Manager window. See **The Chassis Manager Window**, on page 2-18.
- **Chassis Manager Help** brings up a help window with information specifically related to using the Chassis Manager and Device View windows.
- **About Chassis Manager** brings up a version window for the Chassis Manager application in use.

The Module Menu

The Module menu for the MultiSwitch 700 module provides mostly bridging-related selections, many of which are also available from the Bridge Status window:

- **Module Information** opens a Module Information window that provides firmware and manufacturing information which may be useful when troubleshooting any problems that you are having with the module. For more information, refer to **The Module Information Window**, on page 2-19.
- **Module Type** brings up a window containing a description of the selected module; see **Viewing Hardware Types**, on page 2-20.

- **Bridge Status** opens a window that provides an overview of bridging information for each port, and allows you to access all other bridge-related options. Refer to the **Bridging** chapter in the ***Tools Guide*** for more information.
- **Broadcast Suppression** allows you to set a threshold on the number of broadcast packets issued from each port on the MultiSwitch 700 module when it is operating in traditional switch (bridge) mode.
- **Device Find Source Address** enables you to determine through which interface a specified MAC address is communicating by searching the repeater Source Address Table (SAT) and the 802.1d bridge Filtering database. If the specified MAC address is located, a list of interface(s) through which the given address is communicating will be displayed. See **Using Device Find Source Address**, on page 2-27
- **Performance Graph** visually displays the combined performance of all bridging interfaces installed in the MultiSwitch 700 module; refer to the **Bridging** chapter in the ***Tools Guide*** for more information.
- **Spanning Tree** allows you to set bridge parameters when it is operating using the Spanning Tree Algorithm (STA) — the method that bridges use to decide the controlling (root) bridge when two or more bridges are in parallel. Refer to the **Bridging** chapter in the ***Tools Guide*** for more information.
- **SmartTrunk** invokes the SmartTrunk Configuration and Status Screen, which enables you to group interfaces logically to achieve greater bandwidth between devices, if both devices support the SmartTrunk feature. There is no limit to the number of ports that can be included in a single “trunk,” nor is there a limit to the number of trunked “instances” that can be supported. Refer to the **Bridging** chapter in the ***Tools Guide*** for more information.
- **Filtering Database** lets you see and configure the contents of the 802.1d bridge Static and Filtering Databases. Refer to the **Bridging** chapter in the ***Tools Guide*** for more information.
- **Duplex Modes** allows you to set Duplex Mode operation for standard Ethernet interfaces.
- **Enable/Disable Bridge** enables or disables bridging across every interface installed in the MultiSwitch 700 module.

The Port Menus

Each port menu offers the following selections:

- **Connection Type** displays a text description of the connection type of the selected interface. This menu option appears if the device supports the *ctIfConnectionType* OID. See **Viewing Hardware Types**, page 2-20, for details.
- **Description** displays a text description of the selected port. See **Viewing Hardware Types**, on page 2-20, for details.

- **Performance Graph** brings up windows that visually display bridging performance at the selected interface; refer to the **Bridging** chapter in the ***Tools Guide*** for more information.
- **Source Addressing** allows you to view the source MAC addresses communicating through the currently selected interface.
- **I/F Statistics** launches a window that displays MIB-II interface statistics for the selected interface. See Chapter 3, **Statistics**, for more information.
- **Configuration** allows you to configure Ethernet ports for Standard or Full Duplex Mode, or configure operational parameters for Fast Ethernet ports, depending on the type of interface selected.
- **Alarm Configuration** launches the RMON-based Basic and Advanced Alarm applications; see Chapter 4, **Alarm Configuration**, for details. This selection is available for all bridge port interfaces — even those (like ATM) that do not specifically support RMON functionality — as long as at least one Ethernet or Fast Ethernet port is on the module.
- **Statistics** launches the highest level of statistics currently available for the selected port. For standard Ethernet and Fast Ethernet ports, RMON statistics will be displayed if the RMON Default MIB component is active; if it has been disabled, MIB-II interface statistics will display. See Chapter 3, **Statistics**, for more information.
- **Enable/Disable** Port activates or disables bridging for the selected port, respectively; refer to the **Bridging** chapter in the ***Tools Guide***, and **Enabling and Disabling Ports**, on page 2-74, for more information.

Port Status Displays

When you open the Logical View of the chassis, each port will display its current bridging state (defined below) by default; to change this status display, select one of the options on the Port Status menu, as described in the following sections.

Selecting a Port Status View

To change the status view of your ports:

1. Click on **Port Status** on the menu bar at the top of the Device View window; a menu opens.
2. Drag down (and to the right, if necessary) to select the status information you want to display. The port text boxes will display the appropriate status information.

Port status view options are:

Status

You can view four port status categories, as follows:

- **Bridge** — FWD, DIS, LRN, LIS, BLK, or BRK
- **Bridge Mapping** — the instance of the physical interface associated with a bridge port
- **Admin** — ON or OFF
- **Operator** — ON or OFF

If you have selected the **Bridge** status mode, a port is considered:

- FWD (Forwarding) if the port is on-line and ready to forward packets across the MultiSwitch 700 from one network segment to another. Note that this is also the default display for ports which are administratively enabled but not connected.
- DIS (Disabled) if bridging at the port has been disabled by management; no traffic can be received or forwarded on this port, including configuration information for the bridged topology.
- LIS (Listening) if the port is not adding information to the filtering database. It is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move to the forwarding state.
- LRN (Learning) if the Forwarding database is being created, or the Spanning Tree Algorithm is being executed because of a network topology change. The port is monitoring network traffic, and learning network addresses.
- BLK (Blocking) if the port is on-line, but filtering traffic from going across the MultiSwitch 700 from one network segment to another. Bridge topology information will be forwarded by the port.
- BRK (Broken) if the physical interface has malfunctioned.

If you have selected the **Bridge Mapping** status mode, the port display will alter to show the *dot1dBasePortIfIndex*, which is the value of the instance of the interface index (the MIB II *ifIndex*) that corresponds to each bridge / switch port on the device. For a MultiSwitch 700 module, the *dot1dBasePortIfIndex* of the bridge interfaces will map directly to the *ifIndex*.

If you have selected the **Admin** status mode, a port is considered:

- ON if the port is enabled by management.
- OFF if it has not been enabled or if it has been disabled through management action.

The Admin state reflects the state *requested* by management; depending on the circumstances, this may or may not match the current Operator status, described below.

If you have selected the **Operator** status mode, a port is considered:

- ON if the port is currently forwarding packets.
- OFF if the port is not currently forwarding packets.

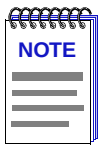
Note that the Operator status provides the *actual* status of the port; depending on the circumstances, this may or may not reflect the Admin state currently *requested* by management. For example, ports which are administratively ON but not yet connected would display an Operator status of OFF, since no packets are being forwarded.

Load

If you choose **Load**, the interface text boxes will display the percentage of network load processed by each port during the last polling interval. This percentage reflects the network load generated per polling interval by devices connected to the port compared to the theoretical maximum load (10, 100, 155.5, 800, or 1000 Mbps) of the connected network.

Errors

If you choose the **Errors** mode, the interface boxes will display the percentage of the total number of valid packets processed by each port during the last polling interval that were error packets. This percentage reflects the number of errors generated during the last polling interval by devices connected to that port compared to the total number of valid packets processed by the port.



The polling interval is set using the Device Management page of the Options window, accessed via the ***Tools —> Options*** *selection from the main menu bar. Refer to the* **User's Guide** *for information on setting node polling intervals.*

I/F Mapping

If you choose the I/F Mapping mode, the interface boxes will display the interface number (*ifIndex*) associated with each port on the MultiSwitch 700 module.

I/F Speed

If you choose the I/F Speed mode, the interface boxes will display the bandwidth of each individual port on the MultiSwitch 700 module: 10M (megabits) for standard Ethernet; 100M for Fast Ethernet, 155.5 M for ATM, 800M for a backplane interface, and 1.00 G for Gigabit Ethernet.

I/F Type

If you choose the I/F Type mode, the interface boxes will display the network type supported by each interface on the MultiSwitch 700 module, e.g., Eth (ethernet-csmacd), ATM, or FDDI. Note that there is no type distinction between standard Ethernet, Fast Ethernet, and Gigabit Ethernet.

Port Status Color Codes

Three of the Port Status display options — Bridge, Admin, and Operator — incorporate their own color coding schemes: for the Bridge option, green = FWD, blue = DIS, magenta = LIS or LRN, orange = BLK, and red = BRK; for Admin and Operator, green = ON, red = OFF, and blue = N/A (not available).

For all other Port Status selections — Bridge Mapping, Load, Errors, I/F Mapping, I/F Speed, and I/F Type — color codes will continue to reflect the most recently selected mode which incorporates its own color coding scheme.

The Chassis Backplane View

By default, the Device View window displays the Logical View of the DLM6C-AA Chassis and an installed MultiSwitch 700 module. The Logical View provides port status information and access to device-, module-, and port-level menus, as described above. You can also display the Chassis Backplane View. The Chassis Backplane View of the hub indicates the five point-to-point backplane connections between the monitored MultiSwitch 700 module and other modules in the chassis. The Backplane View also lets you disable those backplane connections.

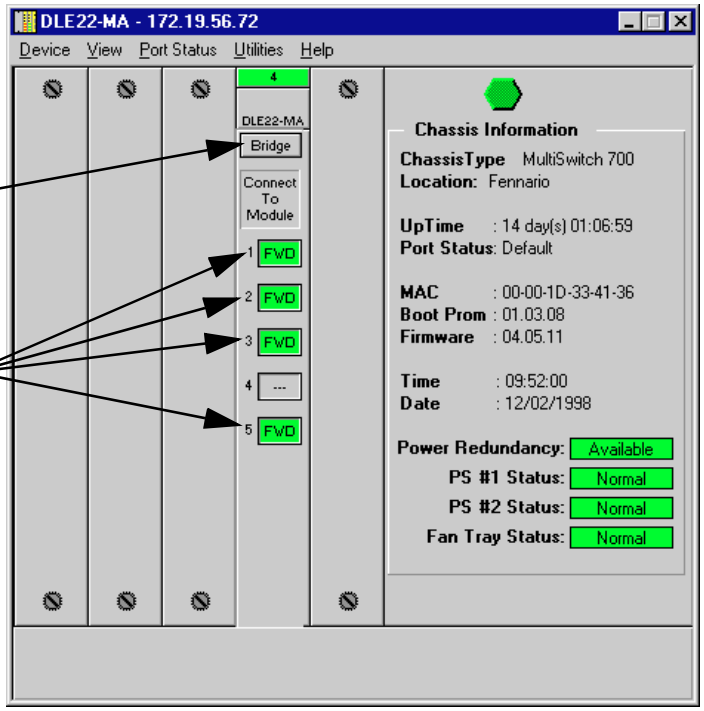
The Chassis Backplane View, Figure 2-5, indicates the operational status of the five point-to-point backplane connections between the monitored MultiSwitch 700 module and other modules in the chassis slots. It also lets you enable or disable the backplane connections to other modules in the chassis.

To access the Chassis Backplane View:

1. Click on **View** in the menu bar to access the View menu.
2. Select **BackPlane Config**. The Chassis Backplane View, Figure 2-5, opens.

*From the **Backplane View** you can display the device interfaces with respect to their bridging status or their MIB II Interface status. The currently selected Port Display Form is shown in the label above the interfaces.*

Below the Port Display Form label, the interfaces appear according to the currently selected Display Form. In the Bridge display form, you can access management options for the individual interfaces.



*To change the display form between **Bridge** and **Interface**, click on the label and select the desired display form from the resulting menu. **Bridge** is the default display form.*

*When the display form is in **Bridge** mode, clicking on an interface will result in a menu, offering various options applicable to the selected backplane interface. For information on enabling or disabling the interface using the **Enable...** or **Disable...** options, see **Enabling or Disabling a Backplane Interface**, on page 2-18. For details on the remaining menu options, refer to their entries in **The Port Menus**, on page 2-11.*

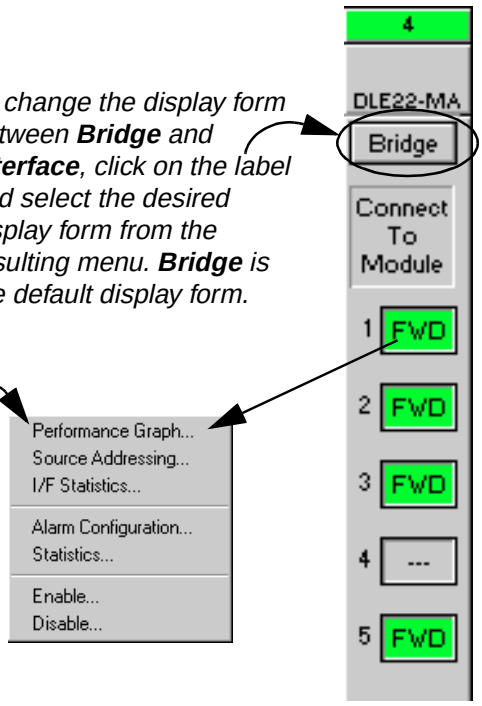


Figure 2-5. The MultiSwitch 700 Module Backplane Device View

The backplane connections are indexed 1–5, where 1 indicates the connection to first slot in the chassis and 5 indicates the connection to the last slot.

Backplane View Bridge Display Form

When the Backplane View display form is in the default **Bridge** mode, each connection is represented by a color-coded text field as follows:

FWD (Green)	The interface is on-line and ready to forward packets across the MultiSwitch 700 from one module to another.
DIS (Blue)	Bridging at the interface has been disabled by management; no traffic can be received or forwarded on this interface, including configuration information for the bridged topology.
LIS (Magenta)	The interface is not adding information to the filtering database. It is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move to the forwarding state.
LRN (Magenta)	The Forwarding database is being created, or the Spanning Tree Algorithm is being executed because of a network topology change. The interface is monitoring network traffic, and learning network addresses.
BLK (Orange)	The interface is on-line, but filtering traffic from going across the MultiSwitch 700 from one module to another. Bridge topology information will be forwarded by the interface.
BRK (Red)	The interface has malfunctioned.

Backplane View Interface Display Form

When the Backplane View is in Interface mode, each connection is represented by a color-coded text field that indicates a combination of the interface's Administrative status, Operational status, and Link status.

The following status conditions are supported:

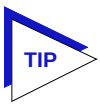
UNK (Gray)	NetSight Element Manager cannot determine the backplane interface's Administrative, Operational, or Link status.
ON (Green)	The backplane interface is operational (up) and administratively enabled. Link status is linked, or not applicable to the interface.

ON (Yellow)	The backplane interface is operational (up) and administratively enabled; however, the interface link status is Not Linked (NLK).
OFF (Blue)	The interface is not operational, and prior to going down it was also administratively disabled.
OFF (Red)	The interface is not operational, but prior to going down it was in an administratively enabled state.
TEST (Magenta)	The interface is in some test operational state.
--- (Gray)	The backplane interface is that associated with the slot in which the currently monitored MultiSwitch 700 module is installed.

Enabling or Disabling a Backplane Interface

You can enable or disable a backplane interface as follows:

1. With the display form in **Bridge** mode, click on the backplane interface which you wish to enable or disable. A menu opens.
2. Select **Enable** or **Disable**, as desired.



The MultiSwitch 700 firmware will not allow you to disable the operational status of an interface supporting your active network connection. This applies to both backplane and front panel interfaces. If you attempt to disable the backplane interface to the module that is supporting your active network connection, you will receive a SET FAILED message.

The Chassis Manager Window

The MultiSwitch 700 modules draws its functionality from a collection of proprietary MIBs and IETF RFCs, and organizes the MIB data into a series of components. A MIB component is a logical grouping of MIB data, and each group controls a defined set of objects. For example, MultiSwitch 700 module bridging information is organized into its own component; Local Management (LIM) and RMON are also contained in separate components. There is no one-to-one correspondence between MIBs and MIB components; a single MIB component might contain objects from several different proprietary MIBs and RFCs.

The Chassis Manager window, Figure 2-6, is a read-only window that displays the MIBs and the MIB components — and, therefore, the functionality — supported by the currently monitored device.

To view the Chassis Manager window:

1. Select **Help—>MIBs Supported**. The Chassis Manager window opens.

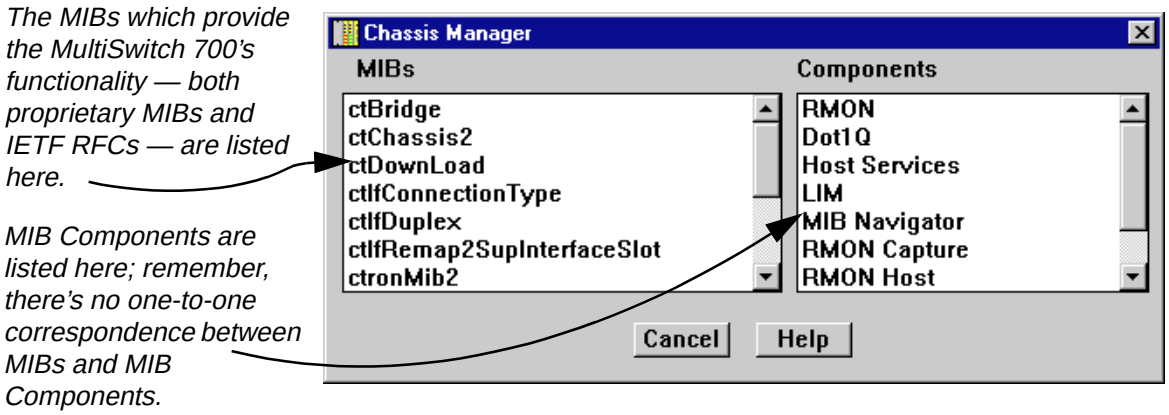


Figure 2-6. The Chassis Manager Window

The Module Information Window

The Module Information window (Figure 2-7) displays system information, as well as data provided by the PIC chip (Product Information Chip). The PIC chip, which is updated each time a module is redesigned, maintains the manufacturing data for the module and stores certain information such as the MAC addresses of various components. Some devices will not return all the data displayed in the Module Information window; these fields will remain blank.

To view the Module Information window:

1. Click on the desired **module index**. The Module menu displays.
2. Select **Module Information**. The Module Information window, Figure 2-7, opens.

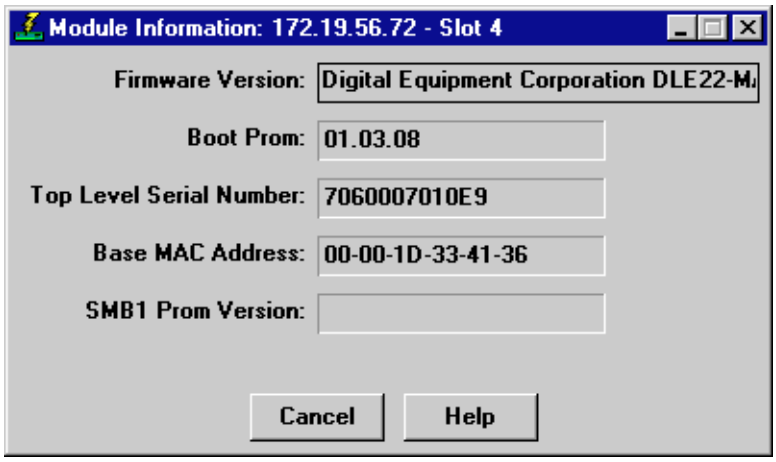


Figure 2-7. The Module Information Window

Firmware Version
The system description of the module, including its firmware revision number.

Boot Prom
The revision of boot PROM firmware in the module, including major version number and minor revision number. The boot PROM provides power-on diagnostics and download capability which enables the module's system image (which provides its runtime functionality) to be downloaded over the network.

Top Level Serial Number
The top level serial number of the module associated with this PIC chip which provides encoded manufacturing date, location, serial number, and top level revision number which can be used for troubleshooting information.

Base MAC Address
The base MAC address (in Ethernet format) assigned to the module.

SMB 1 Prom Version
This field is not applicable to the MultiSwitch 700 module. It will be blank.

Viewing Hardware Types

In addition to the graphical displays described above, menu options available at the device and module levels provide specific information about the physical characteristics of the MultiSwitch 700 hub and its installed modules.

Device Type

Choosing the **Device Type** option on the **Device** menu brings up a window that describes the management device being modeled.

Figure 2-8. Sample Device Type Window

Module Type

From the Module menus on the MultiSwitch 700 Device View window, you can view a description of the Module types installed in your chassis.

1. Click on the desired **module index**. The Module menu displays.

2. Select **Module Type**. A Module Type text box (similar to the example shown in Figure 2-9) opens, describing the module type.

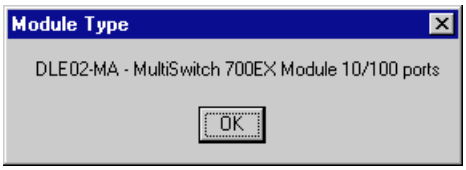


Figure 2-9. Sample Module Type Text Box

Connection Type

If your MultiSwitch 700 supports the ***ctIfConnectionType*** OID, its Port menus will contain the **Connection Type** option. Selecting this option will display a window that describes the selected interface's connection type.

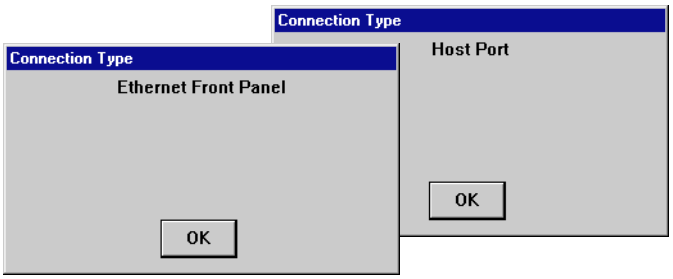


Figure 2-10. Sample Connection Type Windows

Interface Description

Choosing the **Description** option from the Port menu brings up a window that describes the selected interface.

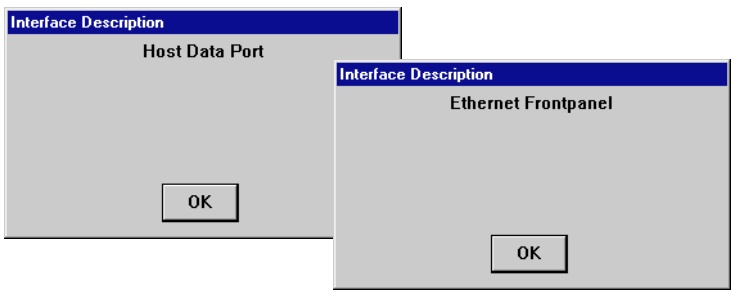


Figure 2-11. Sample Interface Description Windows

Viewing I/F Summary Information

The **I/F Summary** menu option available from the Device menu lets you view statistics for the traffic processed by each network interface on your device. The window also provides access to a detailed statistics window that breaks down Transmit and Receive traffic for each interface.

To access the I/F Summary window:

1. From the Device View, click on the **Device** option from the menu bar.
2. Click again to select **I/F Summary**. The I/F Summary window, Figure 2-12, opens.

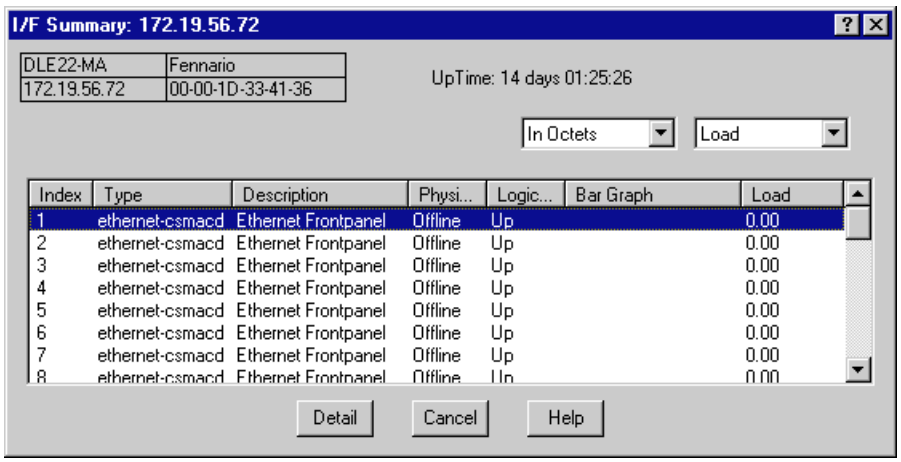


Figure 2-12. The I/F Summary Window

The I/F Summary window provides a variety of descriptive information about each interface on your device, as well as statistics which display each interface's performance.

The following descriptive information is provided for each interface:

Index
The index value assigned to each interface on the device.

Type
The type of the interface, distinguished by the physical/link protocol(s) running immediately below the network layer. Possible values are **fddi** (for an installed DELHF-UA), **ethernet-csmacd** (for standard, Fast Ethernet, and Gigabit Ethernet front panel interfaces, as well as the backplane interfaces to the chassis), **atm** (for an installed DELHA-UA), and **Software LoopBack** for the i960 Host Data port.

Description
A text description of the interface: e.g., **Ethernet Frontpanel** (for the standard Ethernet front panel interfaces), **Fast Ethernet** (for front panel Fast Ethernet interfaces), **FTM Backplane** (for the backplane interfaces to the chassis), **Host** or **Host Data Port** for the on-board i960 Host interface, and **ATM**, or **FDDI**, for an installed modular interface.

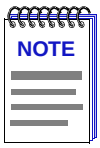
Physical Status
Displays the current physical status — or operational state — of the interface: **Online** or **Offline**.

Logical Status
Displays the current logical status — or administrative state — of the interface: **Up** or **Down**.

Interface Performance Statistics/Bar Graphs

The statistical values (and, where available, the accompanying bar graphs) to the right of the interface description fields provide a quick summary of interface performance. You can select the statistical value you want to display and the units in which you want those values displayed by using the two menu fields directly above the interface display area, as follows:

1. In the right-most menu field, click on the down arrow and select the unit in which you wish to display the selected statistic: **Load**, **Raw Counts**, or **Rate**.



*Bar graphs are only available when **Load** is the selected base unit; if you select **Raw Counts** or **Rate**, the Bar Graph column will be removed from the interface display.*

2. Once you have selected the base unit, click on the down arrow in the left-most field to specify the statistic you'd like to display. Note that the options available from this menu will vary depending on the base unit you have selected.

After you select a new display mode, the statistics (and graphs, where applicable) will refresh to reflect the current choice, as described below.

Raw Counts
The total count of network traffic received or transmitted on the indicated interface since device counters were last reset. Raw counts are provided for the following parameters:

In Octets	Octets received on the interface, including framing characters.
In Packets	Packets (both unicast and non-unicast) received by the device interface and delivered to a higher-layer protocol.

In Discards	Packets received by the device interface that were discarded even though no errors prevented them from being delivered to a higher layer protocol (e.g., to free up buffer space in the device).
In Errors	Packets received by the device interface that contained errors that prevented them from being delivered to a higher-layer protocol.
In Unknown	Packets received by the device interface that were discarded because of an unknown or unsupported protocol.
Out Octets	Octets transmitted by the interface, including framing characters.
Out Packets	Packets transmitted, at the request of a higher level protocol, by the device interface to a subnetwork address (both unicast and non-unicast).
Out Discards	Outbound packets that were discarded by the device interface even though no errors were detected that would prevent them from being transmitted. A possible reason for discard would be to free up buffer space in the device.
Out Errors	Outbound packets that could not be transmitted by the device interface because they contained errors.

Load

The number of bytes processed by the indicated interface during the last poll interval in comparison to the theoretical maximum load for that interface type (10 Mbps for standard Ethernet; 100 Mbps for Fast Ethernet or FDDI; 155.5 Mbps for ATM; 800 Mbps for a backplane port; 1000 Mbps for Gigabit Ethernet). Load is further defined by the following parameters:

In Octets	The number of bytes received by this interface, expressed as a percentage of the theoretical maximum load.
Out Octets	The number of bytes transmitted by this interface, expressed as a percentage of the theoretical maximum load.

When you select this option, a Bar Graph field will be added to the interface display area; this field is only available when **Load** is the selected base unit.

Rate

The count for the selected statistic during the last poll interval. The available parameters are the same as those provided for Raw Counts. Refer to the **Raw Counts** section, page 2-23, for a complete description of each parameter.

Viewing Interface Detail

The Interface Statistics window (Figure 2-13) provides detailed MIB-II interface statistical information — including counts for both transmit and receive packets, and error and buffering information — for each individual port interface. Color-coded pie charts also let you graphically view statistics for both received and transmitted Unicast, Multicast, Discarded, and Error packets.

To open the Interface Statistics window:

1. In the I/F Summary window, click to select the interface for which you'd like to view more detailed statistics.
2. Click on **Detail**. The appropriate I/F Statistics window, Figure 2-13, opens.

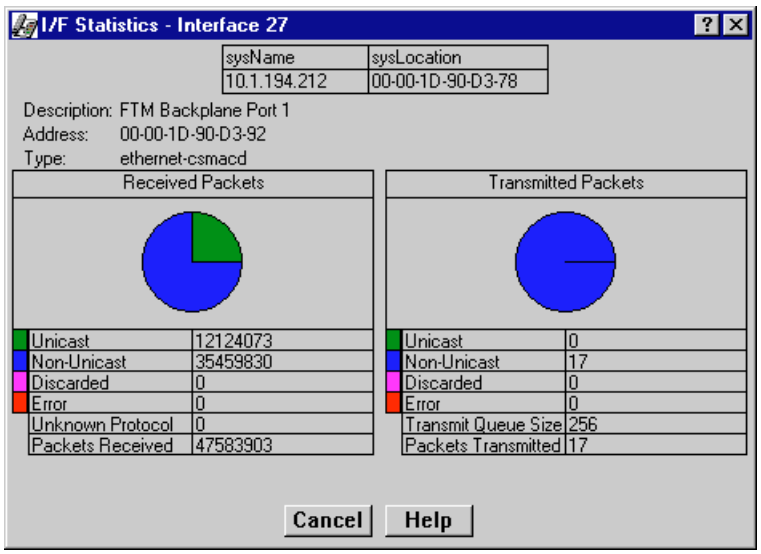


Figure 2-13. Detail Interface Statistics

TIP

*You can also access this information via the I/F Statistics option available on the individual port menus; see Chapter 3, **Statistics**, for more information.*

Three informational fields appear in the upper portion of the window:

Description

Displays the interface description for the currently selected interface (e.g., Enet Port, Fast Enet Port, FDDI, ATM, or Backplane Port).

Address

Displays the MAC (physical) address of the selected interface.

Type
Displays the interface type of the selected port: ethernet-csmacd, fddi, or atm.

The lower portion of the window provides the following transmit and receive statistics; note that the first four statistics are also graphically displayed in the pie charts.

Unicast
Displays the number of packets transmitted to or received from this interface that had a single, unique destination address. These statistics are displayed in the pie chart, color-coded green.

Non-Unicast
Displays the number of packets transmitted to or received from this interface that had a destination address that is recognized by more than one device on the network segment. The multicast field includes a count of broadcast packets — those that are recognized by *all* devices on a segment. These statistics are displayed in the pie chart, color-coded dark blue.

Discarded
Displays the number of packets which were discarded even though they contained no errors that would prevent transmission. Good packets are typically discarded to free up buffer space when the network becomes very busy; if this is occurring routinely, it usually means that network traffic is overwhelming the device. To solve this problem, you may need to re-configure your bridging parameters, or perhaps re-configure your network to add additional bridges or switches.

These statistics are displayed in the pie chart, color-coded magenta.

Error
Displays the number of packets received or transmitted that contained errors. These statistics are displayed in the pie chart, color-coded red.

Unknown Protocol *(Received only)*
Displays the number of packets received which were discarded because they were created under an unknown or unsupported protocol.

Packets Received *(Received only)*
Displays the number of packets received by the selected interface.

Transmit Queue Size *(Transmit only)*
Displays the number of packets currently queued for transmission from this interface. The amount of device memory devoted to buffer space, and the traffic level on the target network, determine how large the output packet queue can grow before the MultiSwitch 700 module will begin to discard packets.

Packets Transmitted *(Transmit only)*
Displays the number of packets transmitted by this interface.

Making Sense of Detail Statistics

The statistics available in this window can give you an idea of how an interface is performing; by using the statistics in a few simple calculations, it's also possible to get a sense of an interface's activity level:

To calculate the percentage of input errors:

Received Errors /Packets Received

To calculate the percentage of output errors:

Transmitted Errors /Packets Transmitted

To calculate the total number of inbound and outbound discards:

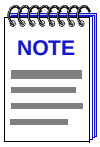
Received Discards + Transmitted Discards

To calculate the percentage of inbound packets that were discarded:

Received Discards /Packets Received

To calculate the percentage of outbound packets that were discarded:

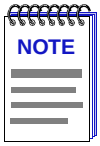
Transmit Discards /Packets Transmitted



*The Interface Statistics window does not offer **Disable** or **Test** options. These options are available in the Interface Group window, which can be accessed via the System Group window (select **System Group** from the **Device** menu). Refer to your* **Generic SNMP User's Guide** *for information on the System Group and Interface Group windows.*

Using Device Find Source Address

When you select the **Device Find Source Address** option, the device's 802.1D Filtering database is searched for the specified MAC address. If it is found, the **Component** field will display the value "Bridge" indicating that the address was found on a bridging interface, and the **Port Instance** field will display the index number assigned to the bridge port on which the address was located.



You may receive an error message stating "Can't Display Source Address" if a Port Instance of "0" or "0.0" is reported. This value indicates that the MAC address is communicating through the backplane instead of through a front panel interface.

The Device Find Source Address window can be accessed from the Chassis View menu or the Module Index:

From the Chassis View:

1. Select **Device—>Device Find Source Address**.

From the Module Index:

1. Click on a **module index** to display the Module menu and select **Device Find Source Address**.

   The Device Find Source Address window, as shown in Figure 2-14, opens.

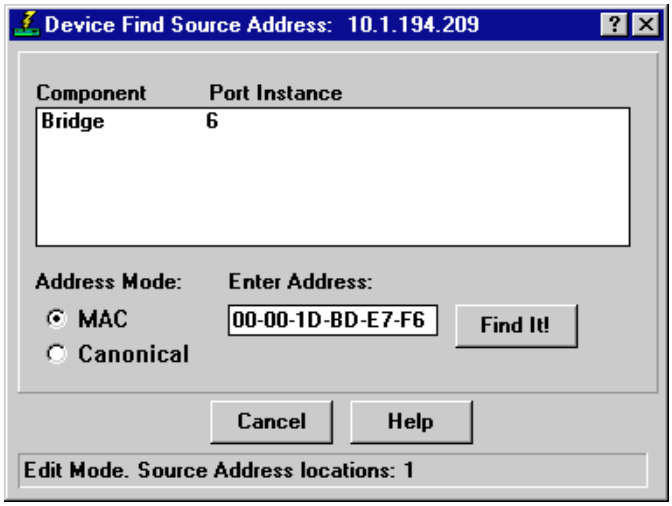


Figure 2-14. Device Find Source Address Window

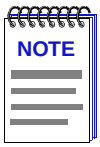
The Device Find Source Address window displays the following information:

Component
Displays the type of interface through which the specified MAC address is communicating. This field will report **Bridge**.

Port Instance
Displays the bridge port index number on which the specified MAC address was found.

To use the Device Find Source Address window:

1. In the **Address Mode** field, select the format of the Source Address you wish to find, either **MAC** or **Canonical**.
2. In the **Enter Address** text box, enter the Source Address you wish to find in the appropriate XX-XX-XX-XX-XX-XX format.

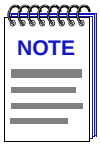


If you enter the MAC format of a specified address, and then click on ***Canonical****, NetSight Element Manager will do the address conversion for you, from the Ethernet hexadecimal format to the Token Ring Canonical format. The same is also true if you enter the Canonical format of a specified address and then select* ***MAC****.*

3. Click on the **Find It!** button. A "**Processing Request**" message displays in the status bar at the bottom of the window.

If the specified MAC address is located, a list of the interface(s) through which the given address is communicating displays in the list box. A status message at the bottom of the window will display the number of interfaces through which the given MAC address is communicating.

If the specified MAC address cannot be found, a "**Source Address not found**" message displays.



*If the MAC address is entered in an incorrect format, an "****Invalid MAC Address. Enter Valid MAC Address****" message displays. Enter the address in the correct XX-XX-XX-XX-XX-XX hexadecimal format.*

Managing the Module

In addition to the performance and configuration information described in the preceding sections, the Device View also provides you with the tools you need to configure your MultiSwitch 700 module and keep it operating properly. Hub management functions include setting operating parameters for Ethernet, FDDI, Fast Ethernet, Gigabit Ethernet, and COM ports; managing an attached UPS; redirecting traffic from one module interface to another; setting port priority parameters; configuring transmission thresholds for broadcast packets; viewing and configuring system resources; setting device date and time; and enabling and disabling bridging at specific port interfaces.

Configuring Ports

The Configuration options available for FDDI, Ethernet, Fast Ethernet, Gigabit Ethernet and COM ports allow you to configure operating parameters specific to each port type: for FDDI and standard Ethernet ports, you can set the Duplex Mode; for Fast Ethernet ports on first generation modules, you can set a variety of duplex mode and negotiation parameters; for Fast Ethernet and Gigabit Ethernet ports on second generation modules you can set speed, duplex mode, and flow control parameters; and for COM ports, you can select the operation you wish the port to perform, and set any associated speed parameters. FDDI, Ethernet, Fast

Ethernet and Gigabit Ethernet Port Configuration windows are available from the Device View Port menus; the COM Port option is available from the Device menu. Note that no configuration option currently exists for ATM ports.

Configuring Standard Ethernet and FDDI Ports

The Port Configuration window available for both standard Ethernet and FDDI ports allows you to set an interface to either Standard or Full Duplex Mode. Full Duplex mode effectively doubles the available wire speed by allowing the interface to both receive and transmit simultaneously. This window will also display the mode currently in effect on the selected interface.

To access the Port Configuration Window:

1. Select the port you wish to configure. The Port Menu will display.
2. Click **Configuration**. The Port Configuration window, Figure 2-15, opens.

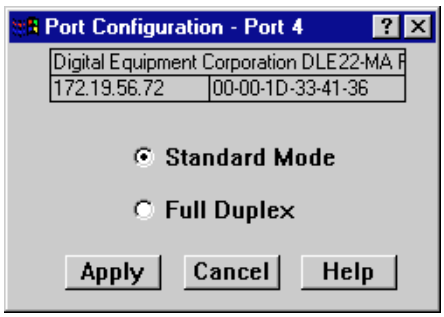


Figure 2-15. The Port Configuration Window

TIP

*If you select the **Configuration** option available for a Fast Ethernet interface, an entirely different window displays; see **Configuring Fast Ethernet Ports on First Generation Modules**, on page 2-31, or **Configuring Ethernet Ports on Second Generation Modules**, on page page 2-36, for information on configuring these ports.*

*For standard Ethernet interfaces, Full Duplex should **only** be enabled on an interface that has a connection to a single destination address at the other end of the connection (i.e., it is not a segment with an attached repeater cascading the connection to multiple destination addresses).*

Full Duplex mode disables the collision detection circuitry at the interface, so that both Transmit and Receive wires can be used simultaneously. With a single destination address at the other end of the connection (for example, if the connection was to a full duplex interface on another switching module, or if a single file server was connected to the full duplex switch port), this essentially doubles the available bandwidth from 10 Mbit/sec to 20 Mbit/sec. The interface at the other end of the connection must also have Full Duplex enabled at the attached interface.

*Full Duplex mode **must** be disabled if the interface is communicating with multiple destinations simultaneously (i.e., if a repeater is cascaded from the interface), since Ethernet relies on Collision Sense for proper operation.*

*Similarly, an FDDI Full Duplex connection must also only be run point-to-point between two supporting FDDI interfaces (e.g., another DELHF-UA), since the dual bandwidth is attained by running data on both primary and secondary paths simultaneously. Since Full Duplex overrides standard FDDI protocol (and eliminates ring redundancy), it will not operate in a "ring" configuration, but only as a point-to-point high speed data trunk between hubs. You must use Local Management to configure your DELHF-UA for Full Duplex operation **prior** to making physical connections. Refer to your Local Management Guide for more information.*

Use the options in this window to select the desired mode:

Standard Mode
In Standard Mode, an interface can only either transmit *or* receive at any given time, and must wait for one activity to be completed before switching to the next activity (receive or transmit). In this mode, standard wire speeds (10 Mbps for Ethernet, 100 Mbps for FDDI) are available.

Full Duplex
In Full Duplex Mode, an interface can both receive *and* transmit packets at the same time, effectively doubling the available wire speed to 20 Mbps (for Ethernet) or 200 Mbps (for FDDI).

Be sure to click on **Apply** to set your changes; note that the interface's current mode can be determined by the field selected in the window.

Configuring Fast Ethernet Ports on First Generation Modules

The Port Configuration window available for Fast Ethernet ports on first generation modules (e.g., a DELF3-UI, DELFX-UI, or DELTX-UI port interface module) allows you to both view and set those ports' available modes. All 100Base-TX Fast Ethernet ports can be configured to operate in either standard Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) mode, and in each mode can be

configured to operate in Full Duplex, effectively doubling the available wire speed (from 10 to 20 Mbps in standard Ethernet mode, or from 100 to 200 Mbps in Fast Ethernet mode); 100Base-FX (fiber) ports can be configured to operate in their standard 100 Mbps mode, or in Full Duplex mode. This window also displays the mode currently in effect on the selected interface, and provides some information (where it is available) about the interface's link partner.

To access the Port Configuration Window:

1. Select the port you wish to configure; the Port Menu will display.
2. Click **Configuration.** The Fast Ethernet Port Configuration window, Figure 2-16, opens.

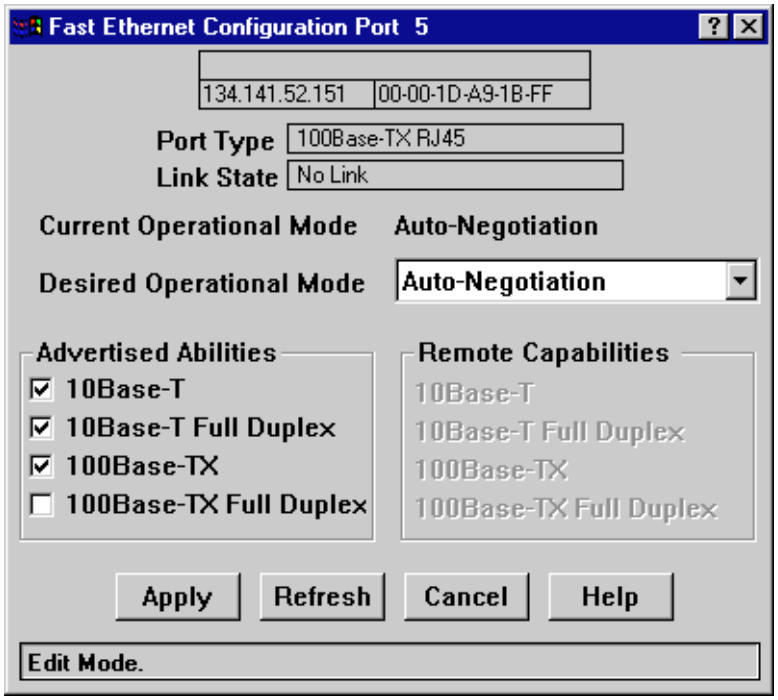


Figure 2-16. The Fast Ethernet Port Configuration Window

NOTE

Auto-Negotiation is not supported by the DELFX-UI Fast Ethernet port interface module. If you launch the window for a port module slot which has no port interface module installed, the Port Type will display as Unknown, the Link State will display No Link, and the rest of the fields will be blank and/or grayed out.

TIP

If you select the Configuration option available for a standard Ethernet or FDDI interface or for a Fast Ethernet port on a second generation module, an entirely different window displays; see ***Configuring Standard Ethernet and FDDI Ports****, on page 2-30, or* ***Configuring Ethernet Ports on Second Generation Modules****, on page 2-36, for information on configuring these ports.*

From this window you can manually set the operational mode of the port, or — for 100Base-TX interfaces — set the port to Auto-Negotiation so that the appropriate operational mode can be determined automatically. The mode you set will determine the speed of the port and whether it uses Full Duplex or Standard Mode bridging.

The window displays the following information about the selected Fast Ethernet port:

Port Type

Displays the port's type: 100Base-TX RJ-45 (for built-in Fast Ethernet ports and the DELTX-UI Fast Ethernet port interface module), 100Base-FX MMF SC Connector (for the DELFX-UI Fast Ethernet port interface module), or Unknown (for a port slot with no module installed).

Link State

Displays the current connection status of the selected port: Link or No Link.

Current Operational Mode

Indicates which of the available operational modes is currently in effect: 10Base-T, 10Base-T Full Duplex, 100Base-TX, 100Base-TX Full Duplex, 100Base-FX, or 100Base-FX Full Duplex. If the port is still initializing, not linked, or if there is no port module installed in the slot, this field will remain blank.

Desired Operational Mode

Displays the operational mode that you have selected for this port, and allows you to change that selection. The following operational modes are available for each port:

100Base-TX Auto-Negotiation, 10Base-T, 10BASE-T Full Duplex, 100Base-TX, and 100Base-TX Full Duplex.

100Base-FX 100Base-FX and 100Base-FX Full Duplex

If you choose to select a specific mode of operation (rather than auto-negotiation), you should be sure that the link partner supports the same mode. Otherwise, no link will be achieved.

If you select a Full Duplex mode and the link partner supports the same wire speed but not Full Duplex, a link will be achieved, but it will be unstable and will behave erratically.

If you select Auto-Negotiation, the local node will try to match the mode of the link partner, even if the link partner is not set to auto-negotiate, and even if the local node must use a mode which it is not currently advertising.

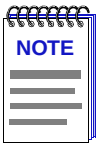
If Auto-Negotiation is the selected mode, the **Current Operational Mode** field will indicate which mode was selected by the link partner. See **Setting the Desired Operational Mode**, on page 2-35, for more information.

Advertised Abilities

For 100Base-TX ports which have been configured to operate in Auto-Negotiation mode, this field allows you to select which of the operational modes available to the port can be selected by the negotiating link partners.

During Auto-Negotiation, each of the link partners will advertise all selected modes in descending bandwidth order: 100Base-TX Full Duplex, 100Base-TX, 10Base-T Full Duplex, and 10Base-T. Of the selected abilities, the highest mode mutually available will automatically be used. If there is no mode mutually advertised, no link will be achieved.

If you have selected a specific operational mode for your 100Base-TX port, the Advertised Abilities do not apply; the selected Advertised Abilities also do not restrict the local node's ability to set up a link with a partner who is not currently Auto-Negotiating.



Auto-Negotiation is not currently supported for 100Base-FX ports.

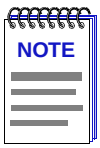
Remote Capabilities

When the local node is set to Auto-Negotiation, this field will display the advertised abilities of the remote link — even if the remote link is not currently set to auto-negotiate. Possible values for this field are:

- 100Base-TX Full Duplex
- 100Base-TX
- 10Base-T Full Duplex
- 10Base-T

- Link Partner does not support Auto-Negotiation — Auto-Negotiation is either not supported by or is not currently selected on the remote port.
- Unknown — the link partner's capabilities could not be determined.

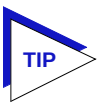
When the local node is ***not*** set to Auto-Negotiation, this field will be grayed out, even if the link partner is set to Auto-Negotiation and is advertising abilities.



If both link partners are set to Auto-Negotiation, but there is no mutually-advertised operational mode, no link will be achieved, and both nodes may display the message "Link Partner does not support Auto-Negotiation." To resolve this situation, be sure both link partners advertise all their abilities, or be sure they advertise at least one mutually-available mode.

Setting the Desired Operational Mode

For any 100Base-TX port, you can specifically choose any one of the four available operational modes, or you can select Auto-Negotiation mode, which allows the port to negotiate with its link partner to find the highest mutually available bandwidth. If you select Auto-Negotiation mode, you must also choose which of the port's bandwidth capabilities you wish to advertise to the link partner.



If you select Auto-Negotiation at both ends of a link, be sure at least one mutually-advertised operational mode is available.

For a 100Base-FX port, the selection process is somewhat simpler; Auto-Negotiation for these ports is not supported at this time, so you need only choose between 100Base-FX standard mode and 100Base-FX Full Duplex. However, you must still be sure that both link partners are set to the same operational mode, or the link will be unstable.

To set your desired operational mode:

1. Click on the **Desired Operational Mode** combo box to display the menu of available options; drag down to select the operational mode you wish to set.

   For 100Base-TX ports, the available options are:

   Auto Negotiation — the operational mode will be dynamically set based on the modes selected in the Advertised Abilities field (where both link partners are auto-negotiating) and the speeds and modes supported by the attached device

   10Base-T — 10 Mbps connection, Standard Mode

   10Base-T Full Duplex — 10 Mbps connection, Duplex Mode

   100Base-TX — 100 Mbps connection, Standard Mode

100Base-TX Full Duplex — 100 Mbps connection, Duplex Mode

For 100Base-FX ports, options are:

100Base-FX — 100 Mbps connection, Standard Mode

100Base-FX Full Duplex — 100 Mbps connection, Duplex Mode

2. If you have selected Auto-Negotiation (for 100Base-TX ports only), use the **Advertised Abilities** field to select the operational capabilities you wish to advertise to the port's link partner. If both link partners will be auto-negotiating, be sure there is at least one mutually-advertised operational mode, or no link will be achieved.

The selected Advertised Abilities only come into play when both link partners are auto-negotiating; if only one link partner is set to auto-negotiate, that node will establish a link at whatever mode its partner is set to, even if that mode is not currently being advertised.

3. Click **Apply** to save your changes. Click **Refresh** to display the new settings. It may take a few minutes for mode changes to be completely initialized, particularly if the link partners must negotiate or re-negotiate the mode; you may need to refresh the window a few times before current operational data is displayed.

Configuring Ethernet Ports on Second Generation Modules

The Ethernet Configuration window available for Fast Ethernet and Gigabit Ethernet ports on second generation modules (e.g., DLE49-MA and DLE52-MA) allows you to both view and set those ports' available speed, modes, and flow control. All second generation modules support the ctEthernetParameters MIB. All Ethernet ports that return at least one instance for a query of the *ctEtherSupportedDuplex* OID will use the Ethernet Configuration window as shown in Figure 2-17.

All 100Base-TX Fast Ethernet ports can be configured to operate in either standard Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) mode, and each mode can be configured to operate in Full Duplex effectively doubling the available wire speed (from 10 to 20 Mbps in standard Ethernet mode, or from 100 to 200 Mbps in Fast Ethernet mode). 100Base-FX (fiber) ports can be configured to operate in their standard 100 Mbps mode, or in Full Duplex mode. 1000Base-SX/LX/CX Gigabit Ethernet ports are always configured to operate in 1000 Mbps, Full Duplex mode.

This window displays the mode currently in effect on the selected interface, and provides some information (where it is available) about the interface's link partner.

To access the Ethernet Configuration Window:

1. Select the port you wish to configure; the Port Menu will display.
2. Click **Configuration.** The Ethernet Configuration window, Figure 2-16, opens.

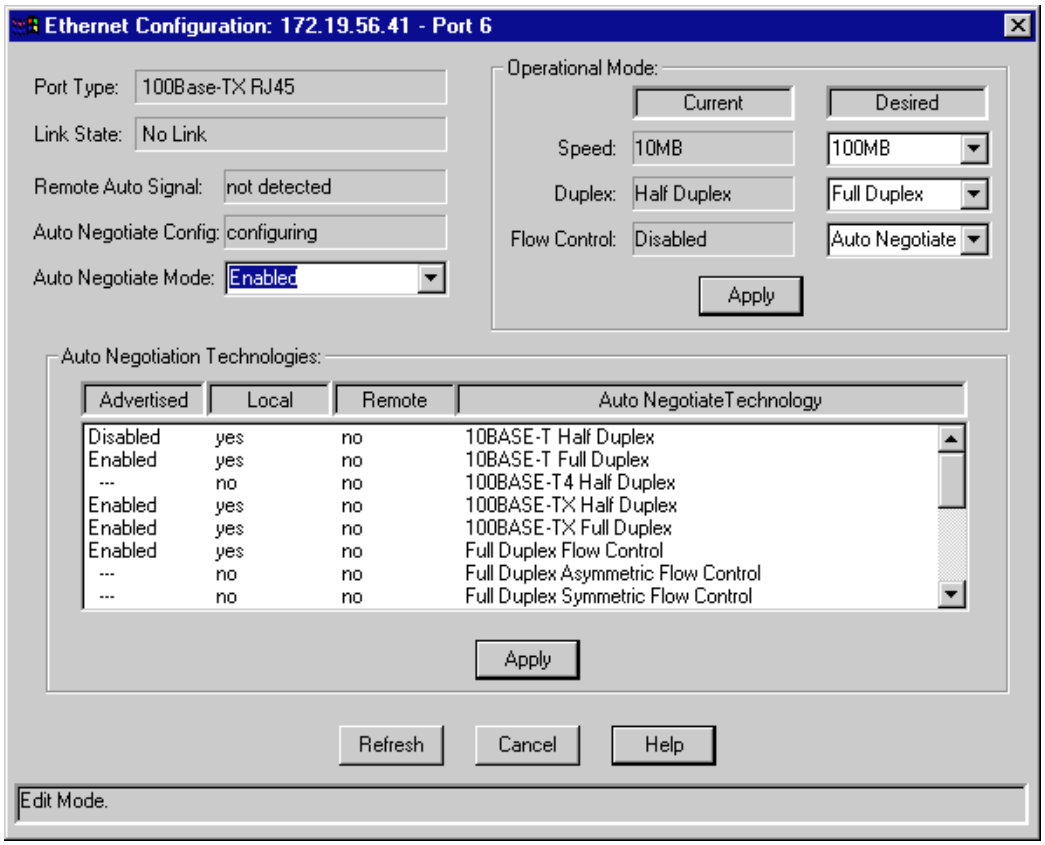


Figure 2-17. The Ethernet Configuration Window

TIP

If you select the Configuration option available for a standard Ethernet or FDDI interface, or for a Fast Ethernet port on a first generation module, an entirely different window displays; see ***Configuring Standard Ethernet and FDDI Ports****, page 2-30, or* ***Configuring Fast Ethernet Ports on First Generation Modules****, page 2-31, for information on configuring these ports.*

From this window you can manually set the operational mode of the port, or — for 100Base-TX and 1000Base-SX/LX/CX interfaces — set the port to Auto Negotiate so that the appropriate operational mode can be determined automatically. The mode you set will determine the port's speed, duplex mode, and flow control.

The window displays the following information about the selected Ethernet port:

Port Type
Displays the port's type: 100Base-TX RJ-45or RJ71 (for built-in Fast Ethernet ports and the FE-100TX Fast Ethernet port module), 100Base-FX MMF SC Connector (for the FE-100FX Fast Ethernet port module), 1000Base-SX/LX/CX (for the VHSIM-G6 Gigabit Ethernet port module), or Unknown (for a port slot with no module installed).

Link State
Displays the current connection status of the selected port: Link or No Link.

Remote Auto Signal
Indicates whether the operating mode at the remote end of the link is set to Auto Negotiate.

Auto Negotiate Config
Indicates whether Auto Negotiate signalling is in progress or has completed. Possible values for this field are: configuring, complete, disabled, parallel detect failed, or other.

Auto Negotiate Mode
Use this field to enable or disable Auto Negotiate for the port. If Auto Negotiate is disabled, the port will use the speed, duplex mode, and flow control settings specified in the Operational Mode fields. Note that 100-BaseFX ports do not support Auto Negotiation; they must use the control settings specified in the Operational Mode fields.

Operational Mode Fields

If the port is *not* set to Auto Negotiate then the settings in the Operational Mode fields are used.

If you choose to select a specific mode of operation (rather than auto negotiation), you should be sure that the link partner supports the same mode. Otherwise, no link will be achieved.

For example, if you select Full Duplex mode and the link partner supports the same wire speed but not Full Duplex, a link will be achieved, but it will be unstable and will behave erratically.

If you select Auto-Negotiation, the local node will try to match the mode of the link partner, even if the link partner is not set to auto-negotiate, and even if the local node must use a mode which it is not currently advertising.

The **Current Operational Mode** settings indicate which of the available operational modes is currently in effect. If Auto Negotiate is the selected mode, the Current Operational Mode fields will indicate which mode was selected by the link partner.

The **Desired Operational Mode** settings display the operational mode that is currently selected for this port, and allows you to change the selection.

The following operational modes can be specified:

Speed
This field specifies a port speed of 10MB, 100MB, or 1000MB.

Duplex
This field specifies Half Duplex or Full Duplex mode for the port.

Flow Control
Flow control allows Ethernet devices to notify attached devices that congestion is occurring and that the sending device should stop transmitting until the congestion can be cleared. There are two commonly used methods of flow control: Frame-based (operates on Full Duplex links) and Backpressure (operates on Half Duplex links).

Ports set to Full Duplex mode have frame-based flow control, using pause control frames. Frame-based flow control options are:

Symmetric The port is able to both receive and transmit pause control frames.

Asymmetric RX This option appears only for Gigabit Ethernet ports. The port will receive pause control frames, but will not transmit its own.

Asymmetric TX This option appears only for Gigabit Ethernet ports. The port is capable of sending pause control frames, but will not acknowledge received pause control frames.

Disabled Disables flow control on the port.

Auto Negotiate Ports configured to operate in auto negotiation mode will only use pause control frames if the negotiation process determines that the link partner supports them. Both ends of the link must support auto negotiation and a common mode of operation.

Ports set to Half Duplex mode use Backpressure flow control. Backpressure flow control simply asserts the carrier sense signal out the port causing the device transmitting to detect a collision, stop transmitting data, and send the jam signal. Backpressure flow control options are enabled or disabled.

Setting the Desired Operational Mode

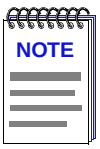
For any 100Base-TX port, you can configure operational modes, or you can select Auto Negotiate mode, which allows the port to negotiate with its link partner to find the highest mutually available bandwidth and flow control. If you select Auto Negotiate mode, you must also choose which of the port's bandwidth and flow control capabilities you wish to advertise to the link partner (refer to **Auto Negotiation Technologies**, page 2-40).

100Base-FX ports do not support auto negotiation for bandwidth or flow control capability, so you must choose between 100Base-FX Half Duplex and 100Base-FX Full Duplex mode, and set the flow control option. However, you must still be sure that both link partners are set to the same operational mode, or the link will be unstable.

For 1000Base-SX / LX / CX ports the speed and duplex modes are always configured at 1000MB Full Duplex. However, you can select Auto Negotiate mode, which allows the port to negotiate with its link partner to find the highest mutually available bandwidth and flow control. If you select Auto Negotiate mode, you must also choose which of the port's bandwidth and flow control capabilities you wish to advertise to the link partner (refer to **Auto Negotiation Technologies**, page 2-40).

To set your desired operational mode:

1. Click on the **Speed, Duplex,** or **Flow Control** list box to display the menu of available options; click to select the operational mode you wish to set.



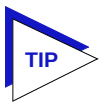
If the port you are configuring does not support Flow Control, the Current Mode field will display "not supported" and the Desired Mode list box will be disabled.

2. Click on the **Apply** button to save your changes.

Auto Negotiation Technologies

For ports which have been configured to operate in Auto Negotiate mode, this list box allows you to select which of the operational modes available to the port will be advertised to the negotiating link partner.

During Auto Negotiation, each of the link partners will advertise all selected modes. Of the selected modes, the highest mode mutually available will automatically be used. If there is no mode mutually advertised, no link will be achieved.



If you select Auto-Negotiation at both ends of a link, be sure at least one mutually-advertised operational mode is available.

If you have manually configured specific operational modes for your 100Base-TX port or if you are configuring a 100Base-FX port, the Auto Negotiation Technologies list box does not apply.

The Auto Negotiation Technologies list box has the following column headings:

Advertised
This column specifies whether the operational mode listed in the far right column of the list box will be advertised to the link partner. Only those operational modes supported by the local port (those with a "yes" listed in the Local column) can be advertised. Valid values are **Enabled** (the mode is supported and will be advertised), **Disabled** (the mode is supported but will not be advertised), and "**---**" (the mode is not supported).

Local
Indicates whether the operational mode listed in the far right column of the list box is supported by the local port.

Remote
Indicates whether the operational mode listed in the far right column of the list box is supported by the remote port.

Auto Negotiate Technology
This column lists possible operational modes.

Setting Advertised Abilities for Auto Negotiation

You can determine which operational mode supported by the local port will be advertised to the negotiating link partner. Of the advertised modes, the highest mode mutually available will automatically be used.

To advertise an operational mode:

1. In the list box, click on the operational mode of choice.

   If the Advertised column had a value of Enabled, it will change to Disabled; a value of Disabled will change to Enabled. If the Advertised column has a value of "---", then the value is not changed.

2. Click **Apply** to save your changes. Click **Refresh** to display the new settings. It may take a few minutes for mode changes to be completely initialized, particularly if the link partners must negotiate or re-negotiate the mode; you may need to refresh the window a few times before current operational data is displayed.

Configuring the COM Port

You can use the COM Port Configuration window (Figure 2-18) to specify the functions that will be performed by the RS232 COM port on the front panel of the monitored MultiSwitch 700 module.

1. Click on **Device** in the Device View menu bar to display the Device menu.
2. Click on **COM Port Configuration** and then right to select **Port 1**. The COM Port Configuration window, Figure 2-18, opens.

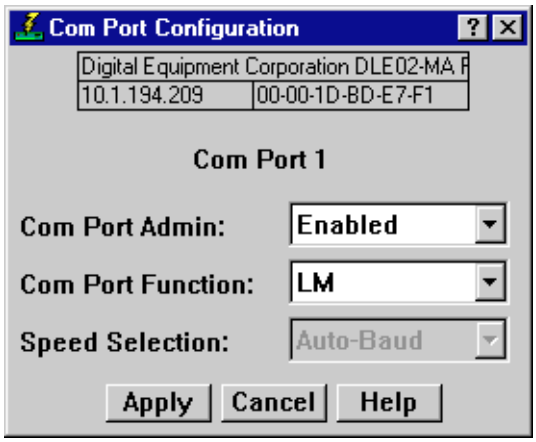


Figure 2-18. The COM Port Configuration Window

You can use the COM Port Configuration window to set the following operating parameters:

COM Port Admin

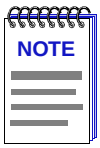
Use this field to administratively enable or disable the COM port.

COM Port Function

Use this field to select the function for which you wish to use the COM port:

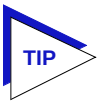
LM	Local Management: select this option if you wish to connect a terminal to the COM port from which to run Local Management.
UPS	Select this option if you wish to connect an uninterruptable power supply (UPS) to the COM Port. Note that if you select this option, an additional option — UPS — displays on the Device menu when you exit and re-enter device management; use the resulting window to configure specific UPS settings.
SLIP	Select this option to use the COM port as a SLIP connection for out-of-band SNMP management via direct connection to a serial port on your network management workstation. Note that when you configure the port as a SLIP connection, you must select the desired baud rate in the **Speed Selection** field described below.

PPP — Select this option to use the COM port as a PPP connection for out-of-band SNMP management via direct connection to a serial port on your network management workstation. Note that when you configure the port as a PPP connection, you must select the desired baud rate in the **Speed Selection** field described below.



Current MultiSwitch 700 firmware versions support only Local Management and UPS via the COM ports; future versions will add SLIP and PPP support. You will receive a SET failed message if you attempt to configure the COM port for SLIP or PPP support.

Speed Selection
If you have configured the selected port as a SLIP or PPP connection, you must select the appropriate baud rate: 2400, 4800, 9600, or 19,200. Note that this field will default to Auto-Baud and become unselectable when the **COM Port Function** is set to LM or UPS.



*If the COM port you wish to configure is currently set to LM or UPS, the **Speed Selection** field will be unavailable until the COM Port Function is set to SLIP or PPP and that change is applied. Once available, the Speed Selection field will default to the last known speed setting; use the down arrow to change this setting if necessary, then click the **Apply** button again to complete the configuration.*

To change the configuration of the selected COM port:

1. Click on ▾ to the right of each field, and select the desired setting.
2. Click on the **Apply** button to save your changes.

Using an Uninterruptable Power Supply (UPS)

Your MultiSwitch 700 supports the use of a UPS (uninterruptable power supply) through its COM port (if configured through local management). (For more information on the use of a UPS with the MultiSwitch 700, consult the MultiSwitch 700 Installation Manual that was included when you purchased the unit.) You can view or change the status of the UPS connected to your MultiSwitch 700 at the UPS window.

Please note that the UPS window will only be active if you currently have a UPS attached to your MultiSwitch 700 through the COM port, and you have correctly set the **Set UPS ID** field.

*Do not set the **Set UPS ID** field unless you have a UPS attached to the MultiSwitch 700, or you will disrupt your use of NetSight Element Manager.*

Accessing the UPS Window

At the UPS window, you can configure the UPS ID model type for the uninterruptable power supply you have attached to the COM port on your device.

You can also view information concerning the UPS connected to your MultiSwitch 700 including:

- The amount of time that your UPS has been running since the last start-up
- The line voltage and battery output
- The actual battery capacity of the UPS (dynamic bar graph)

You can also use a button at the bottom of the window to disconnect your UPS, or you can use the Test option to initiate a self test of the unit.

To access the UPS window:

1. Click on **Device** in the menu bar to access the Device menu.
2. Select **UPS**. The UPS window, Figure 2-19, opens.

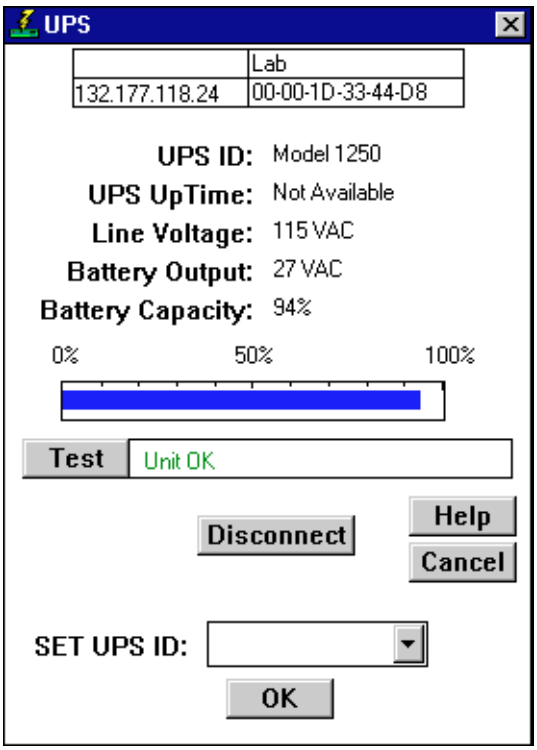


Figure 2-19. The UPS Window

UPS ID

Displays the manufacturer and model typecode of the UPS attached to the COM port of the MultiSwitch 700. You must assign this typecode for the UPS window to be active. (See **Setting the UPS ID**, on page 2-46, for instructions for setting the typecode for your UPS.) The valid typecodes are:

- Model 370
- Model 400
- Model 600
- Model 900
- Model 1250
- Model 2000
- Matrix 3000
- Matrix 5000
- SU 700
- SU 1400
- SU 2000XL
- Other

UPS Uptime

Displays the number of hours that the UPS has been operating since the last time it was started up.

Line Voltage

Displays the voltage coming through the line attached to the MultiSwitch 700.

Battery Output

Displays the amount of battery output voltage.

Battery Capacity

Displays the percentage of remaining battery capacity (100% indicates a fully charged battery).

Test Results

Displays the result of the last self-test performed by the UPS. The possible test results are:

Unit OK	The UPS unit is in working order.
Unit Failed	The UPS unit has failed the self-test. Check the unit for damage or consult your UPS User's Manual.
Bad Battery	The UPS unit battery is bad.
No recent test	No UPS self-test has been performed in the last five minutes.
Unit in test... Please standby	The UPS is currently in test mode.

Setting the UPS ID

You need to set the UPS ID typecode that indicates the manufacturer and model of the UPS.

To set the UPS ID:

1. Click on  next to the SET UPS ID text box. A Model number menu displays. Scroll to highlight the appropriate UPS ID. (Consult the manual that was included when you purchased your UPS for the correct Model ID number.)
2. Click on the **OK** button. The UPS ID you have chosen displays in the text box, and the UPS window will be active.

If your UPS unit does not function after you have set this ID, check the manual you received with the UPS to ensure that you have chosen the correct UPS ID. If you need to change the ID, follow the directions given above.

Using the Test Option

You can use the test option to activate a self-test cycle for your unit. This self-test will check the viability of your unit and its battery.

To activate the test:

1. Click on the **Test** button. The unit will begin its self-test. The results of the test displays in the Test Result text box next to the Test button.

Using the Disconnect Option

You can disconnect the UPS attached to your MultiSwitch 700 through its COM port, as follows:

1. Click on the **Disconnect** button near the bottom of the UPS window. Your UPS will now be disconnected.

To reconnect, click **OK** button, or close, then re-open the UPS window.

Redirecting Traffic on the MultiSwitch 700 Module

The Port Redirector window (Figure 2-20) allows you to redirect traffic from one or more interfaces directly to another interface — essentially mirroring the traffic at the “redirect” interface. This feature is useful in that it allows you to use an external analyzer on the “redirect” port to analyze data, without disturbing the normal switching operations at the original source ports. The Port Redirector window displays the interface remap table and allows you to add new entries to and delete existing entries from this table. When you set a source port to redirect to a destination port, the destination port will transmit out all packets received or transmitted on the source port.

To access the Port Redirector Menu:

1. Click on **Device** in the Device View menu bar to display the Device menu.
2. Select **Port Redirector**. The Port Redirector window, Figure 2-20, opens.

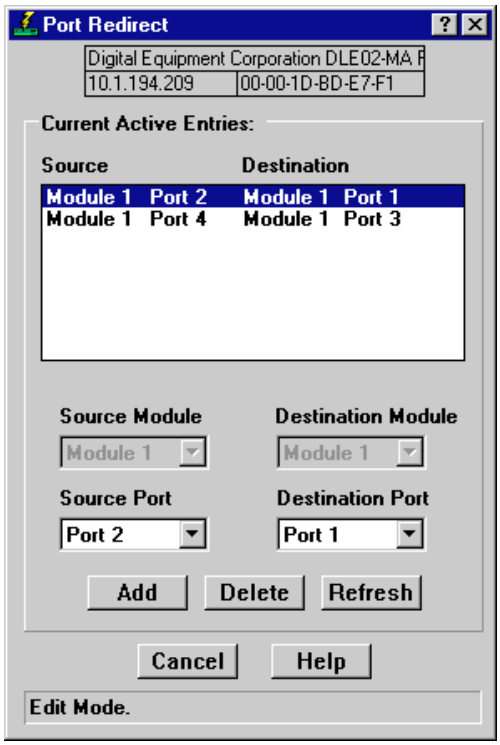


Figure 2-20. The Port Redirector Window

The current port mappings will be listed in this window. You may add entries to or delete entries from this window.

To add an entry:

1. Next to the Source Module display box click on and select the desired source module (**Module X)** from the drop down list.
2. Next to the Source Port display box click on and select the desired source port (**Port X)** from the drop down list.
3. Next to the Destination Module display box click on and select the desired destination module (**Module X)** from the drop down list.
4. Next to the Destination Port display box click on and select the desired destination port (**Port X)** from the drop down list.

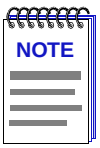
5. Click **Add** to add the redirect pair you have just configured to the list. The new entry will now be displayed in the Current Active Entries list in this window and the port traffic will begin to be redirected.

To delete an entry:

1. Click to highlight the entry line in the Current Active Entries list that you wish to delete.
2. Click **Delete** to remove the redirect pair you have highlighted from the Current Active Entries list. The entry will be deleted from the Current Active Entries list and the traffic from the source port will not be redirected to the destination port any longer.

Priority Configuration

The MultiSwitch 700 modules support priority packet forwarding. Priority packet forwarding lets you designate certain packets to be of higher importance than others, thereby allowing for the forwarding of these packets before packets of lower priority. This functionality is essential for time-critical applications — such as real-time video — on shared networks.



*The **Priority Configuration** menu option will only appear in the **Device** menu for modules that respond to **any** of NetSight Element Manager's queries to the following OIDs: **ctPriorityExtPortStatus**, **ctPriorityExtMaxNumMACEntries**, or **ctPriorityExtNumPktTypeEntries**. If your module's firmware does not respond to these queries, contact the Global Call Center for firmware upgrade information.*

Frame priority is enabled by the "tagging" of MAC frames so that they are given a priority designation when they are forwarded by the MultiSwitch 700 module — which is a tag-aware switch (i.e., one that adheres to the IEEE P802.1p and IEEE P802.1q Draft Standards). Tagging a frame is accomplished by adding a Tag Header to a frame immediately following its original Destination and Source MAC address fields (and any routing fields, if present), and then recomputing the Frame Check Sequence (FCS) appropriately. On receiving such a frame, a tag-aware switch will read the priority from the tagged portion of the frame, remove the Tag Header, recompute the FCS, and then direct it to its appropriate transmission queue.

There are eight priority levels — indicated 0 through 7— available to designate user priority. Frames tagged with a 0 represent the lowest priority level (or normal) traffic, and frames tagged with a 7 indicate the highest priority level traffic.

The MultiSwitch 700 module itself supports two transmission queues: one that is for 0 or normal priority traffic (or any non-tagged traffic), and a second queue that is reserved for frames that have been tagged with a priority level of 1 or higher. On receiving any priority-tagged frames, the MultiSwitch 700 will forward them out of the high priority queue before forwarding any frames in the normal

priority queue. However, the MultiSwitch 700 will tag outgoing frames with the full range of eight priority levels, so that upon reception, a device that supports the entire range of priority queuing will forward the frame appropriately.

You can use NetSight Element Manager to configure the criteria that determine the priority in which frames will be queued for transmission by your MultiSwitch 700 module. Several different criteria can be used to determine a frame's transmission queue order:

- The module and port at which the frame was received.
- The destination and / or source MAC address associated with the frame.
- A combination of destination and / or source MAC address and the frame's protocol type.
- The frame's protocol type.

When you configure the transmission queue for a specific frame, an entry is made in one of three priority tables maintained by the MultiSwitch 700 module. These tables are used to determine which transmit queue to use — normal priority or high priority — when forwarding frames.

- The *ctPriorityExtPortTable* maintains priority entries based on a frame's receive port.
- The *ctPriorityExtMACTable* maintains priority entries based on a frame's MAC-layer information.
- The *ctPriorityExtPktTypeTable* maintains priority entries based on the frame's protocol type.

The following sections discuss how to use the Port Priority Configuration window, the MAC Based Priority Configuration window, and the Frame Priority Configuration window to make entries in these transmit priority tables.

Configuring Priority Queuing Based on Receive Port

You can use the Port Priority Configuration window, Figure 2-21, to determine packet queuing based solely upon the port at which the packet was received. This allows you to ensure that a connected user or LAN segment will have priority when frames that were received on that port are queued for transmission.

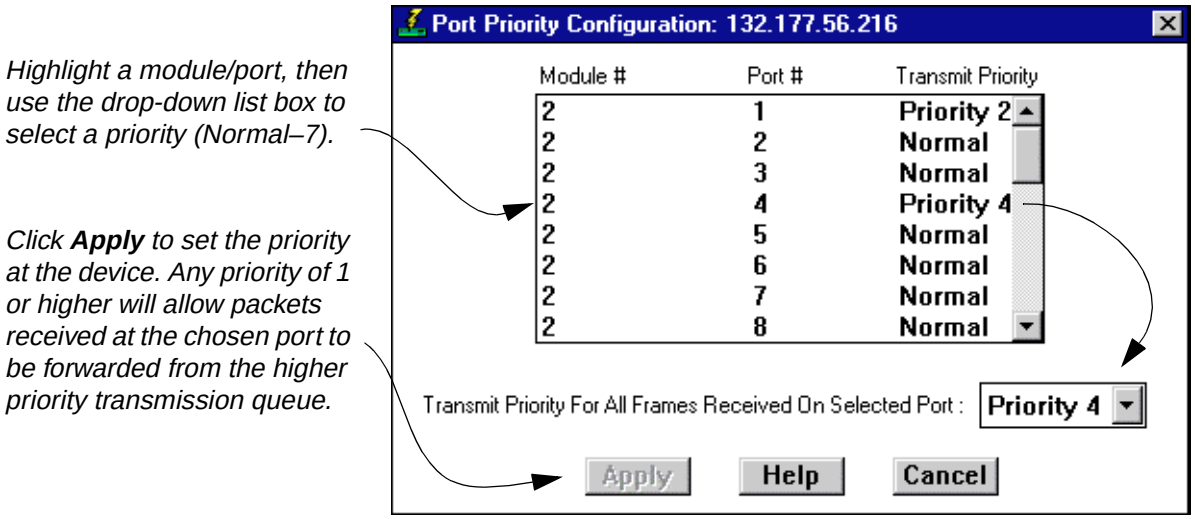


Figure 2-21. The Port Priority Configuration Window

NOTES

In the event that an incoming packet received on a designated port already has a priority associated with it, you can use the ***ctPriorityExtPortFwdInboundPriority*** *OID to determine whether the incoming priority should remain intact, or be replaced with the priority that you have set for the receiving port.*

Use the MIB Tools utility suite to set the ***ctPriorityExtPortFwdInboundPriority*** *OID to 1 (for the appropriate port instance) if you want the incoming packet to retain its originally set priority when received by the port; set the OID to 2 if you want the packet to take the default priority set for the receiving port. Refer to the* **NetSight Element Manager Tools Guide** *for information on using the MIB Tools suite.*

To access the Port Priority Configuration window:

1. Click on **Device** to access the Device menu.
2. Click on **Priority Configuration** and then right to select **Port Based** from the menu. The Port Priority Configuration window opens.

The Port Priority Configuration window displays the contents of the *ctPriorityExtPortTable*. It has a list box that displays the front panel interfaces supported by the MultiSwitch 700 module, along with the slot number occupied by the module, and any transmit priority that has been assigned to those interfaces.

To assign a transmit priority to a port:

1. Click to highlight the port interface of interest in the **Port #** column. Each interface is identified by its MIBII IfIndex.

2. Click on the **Transmit Priority** drop-down list box, and scroll to select the desired priority level (**Normal–7**) for forwarding packets received on the selected port.

NOTE

Remember, since the MultiSwitch 700 module has two transmit queues, a priority of Normal will cause packets received on that port to be forwarded through the lower priority queue, and any priority of 1 through 7 will cause the packets to be forwarded through the higher priority queue. However, other tag-aware switches may use the full range of eight priority queues — so the priority that you assign may have bearing on how the frame is forwarded when it is received by another device.

3. Click the **Apply** button. The defined priority displays next to the port in the Transmit Priority column.

Configuring Priority Queuing Based on MAC-layer Information

You can use the MAC Based Priority Configuration window, Figure 2-22, to determine packet queuing based upon the packet's Source and / or Destination MAC address, as well as the packet's frame Type. These priority entries, based on the frame's MAC-layer information, are maintained in the *ctPriorityExtMACTable*. You can create up to 1024 priority entries for queuing frames based upon on MAC-layer information.

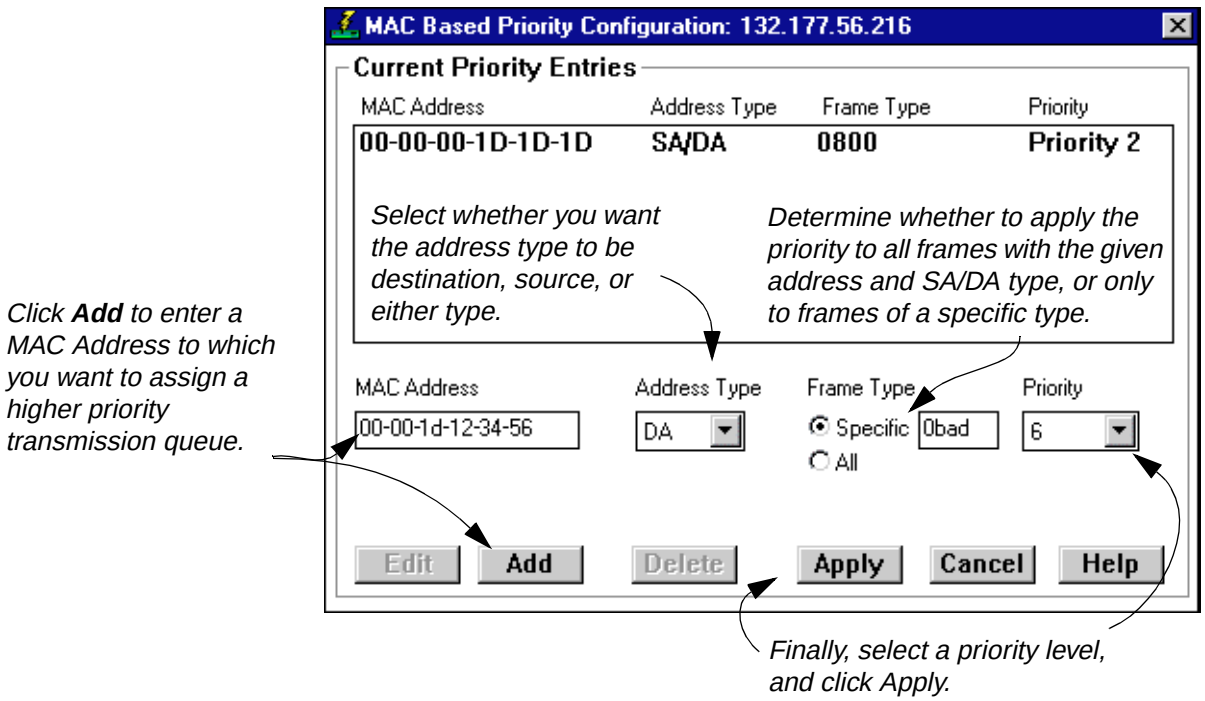


Figure 2-22. The MAC Based Priority Configuration Window

To access the MAC Based Priority Configuration window:

1. Click **Device** to access the Device menu.
2. Click **Priority Configuration**, and then right to select **MAC Based** from the menu. The MAC Based Priority Configuration window opens.

The MAC Based Priority Configuration window contains the following information.

Current Priority Entries

The Current Priority Entries list box displays any MAC-based priority entries that have been configured for the MultiSwitch 700 module. It has four columns:

- MAC Address, which identifies the physical address for which a frame transmit priority entry has been configured.
- Address Type, which identifies whether the address of interest is in the source or destination field, or in both fields, of the frame.
- Frame Type, which indicates whether all frames with the given address will have a transmit priority, or whether a specified frame Type will be used in combination with the address.
- Priority, which displays the current transmit priority assigned to the entry.

Below the Current Priority Entries list box, several text fields and command buttons allow you to configure or edit MAC-based priority entries:

MAC Address

This text field allows you to enter a new MAC address that will have a transmit priority associated with it.

Address Type

This drop-down list box allows you to select whether the given MAC address must be in the source address portion of the frame (SA), the destination address portion (DA), or in either portion (SA / DA).

Frame Type

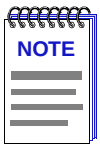
This option button / text box combination allows you to choose whether **All** frame Types with the given address will be given priority, or whether frames of a **Specific** type (as defined in the associated text box) will be given priority.

Priority

Priority, which indicates the transmit priority level assigned to the configured entry.

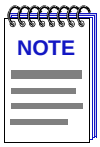
To assign a transmit priority based on MAC-layer information:

1. Click on the **Add** button. The entry fields will be activated.
2. Click in the **MAC Address** text box, and type in the physical address in XX-XX-XX-XX-XX-XX format, where X is a valid hexadecimal value (A-F or 0-9), for which you want to configure a transmit priority.
3. Click on the **Address Type** drop-down list box, and select whether you want the specified address to be in the Source Address portion of the frame (**SA**), the Destination Address portion (**DA**), or in either portion (**SA/DA**).
4. Specify a **Frame Type** that you want associated with the frame:
   a. Click on the appropriate Frame Type option button: **Specific** if you want a certain Frame Type associated with the given MAC address, or **All** if you do not care about the Frame Type.
   b. If you select Specific, click in the associated text box and type in the two-byte hexadecimal value for that protocol type (e.g., 0BAD for Banyan frames).



When creating priority entries, you can specify up to four Frame Types for the same MAC Address value.

5. Click on the **Priority** drop-down list box, and scroll to select the desired priority level — **Normal (0)–7 —** for forwarding packets received with the specified MAC-layer information.



Since the MultiSwitch 700 module has two transmit queues, a priority of Normal will cause packets to be forwarded through the lower priority queue, and any priority of 1 through 7 will cause the packets to be forwarded through the higher priority queue.

6. Click **Apply**. The Current Priority Entries list box will be updated with the newly created entry.

You can edit an existing address entry by changing the priority currently associated with the entry. To do so:

1. Highlight the desired entry in the Current Priority Entries list box, and click on the **Edit** button. The Priority drop-down list box will be activated. (All other parameters will remain grayed-out, since they cannot be edited once they are initially configured).

2. Click on the **Priority** drop-down list box, and scroll to select the new priority level (**Normal–7**) for forwarding packets received with the specified MAC-layer information.

3. Click **Apply**. The Current Priority Entries list box will be updated with the newly edited entry.

To clear a priority entry from the *ctPriorityExtMACTable*:

1. Highlight the desired entry in the Current Priority Entries list box, and click **Delete**. The entry fields will be cleared from the table.

Configuring Priority Queuing Based on Packet Type

You can use the Frame Priority Configuration window, Figure 2-23, to determine packet queuing based solely upon its Type field data. Frame type entries are maintained in the *ctPriorityExtPktTypeTable*. You can configure up to 15 frame Type priority entries for the device.

*Click **Add** to activate the Frame Type field, then type in the 2 byte hexadecimal frame Type.*

Use the drop-down list box to select a priority (Normal–7) associated with that frame Type

*Click **Apply** to set the priority at the device. Any priority of 1 or higher will allow packets received at the chosen port to be forwarded from the higher priority transmission queue.*

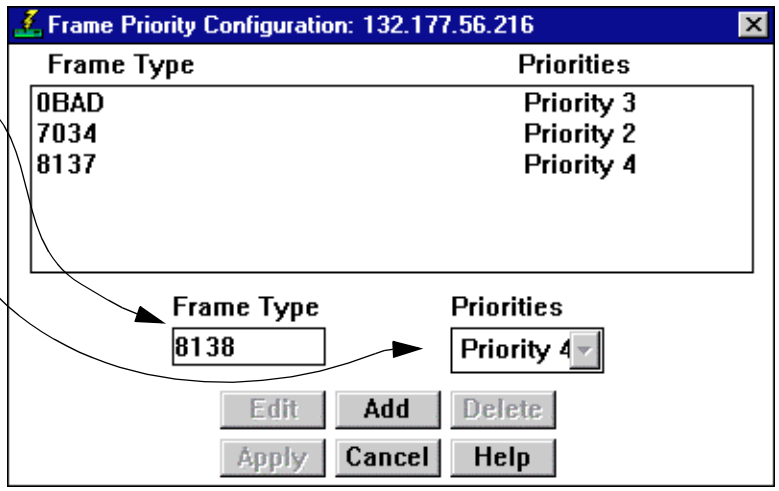


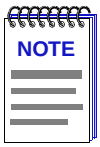
Figure 2-23. Frame Priority Configuration Window

To assign a transmit priority based on frame Type information:

1. Click on the **Add** button. The entry fields will be activated.

2. Click in the **Frame Type** text box, and type in the 2-byte frame Type in XXXX format, where X is a valid hexadecimal value (A-F or 0-9), for which you want to configure a transmit priority (e.g., 8137 for Novell Type 1 frames).

3. Click on the **Priority** drop-down list box, and scroll to select the desired priority level (**Normal–7**) for forwarding packets received with the specified Type field information.



Since the MultiSwitch 700 module has two transmit queues, a priority of Normal will cause packets to be forwarded through the lower priority queue, and any priority of 1 through 7 will cause the packets to be forwarded through the higher priority queue.

4. Click **Apply**. The Frame Type Entries list box will be updated with the newly created entry.

You can edit an existing frame Type entry by changing its previously assigned priority.

1. Highlight the desired entry in the Current Priority Entries list box, and click on the **Edit** button. The Priorities drop-down list box will be activated (the Frame Type cannot be edited once it is initially configured).
2. Click on the **Priority** drop-down list box, and select the desired priority level (**Normal–7**) for forwarding packets received with the specified frame Type information.
3. Click **Apply**. The Frame Type Priorities Entries list box will be updated with the newly edited entry.

To clear a priority entry from the *ctPriorityExtPktTypeTable*:

1. Highlight the desired entry in the Frame Type Priorities Entries list box, and click **Delete**. The entry fields will be cleared from the table.

Broadcast Suppression

From the Broadcast Statistics and Suppression window, you can monitor broadcast peak statistics, and suppress the amount of broadcast frames received on each interface on your MultiSwitch 700 module (thereby protecting your network from broadcast storms). Specifically, you can monitor the number of frames each interface is receiving, and set limits on how many of those broadcast frames will be forwarded to the other interfaces. Once a threshold has been reached on an interface, broadcast frames will be dropped. From the Broadcast Statistics and Suppression window, you can set a unique threshold for each interface on a frames per second basis.

To access the Broadcast Statistics and Suppression window:

1. Click on the **module index** of the module of interest to display the Module menu.
2. Select **Broadcast Suppression**. The Broadcast Statistics and Suppression window, Figure 2-24, opens.

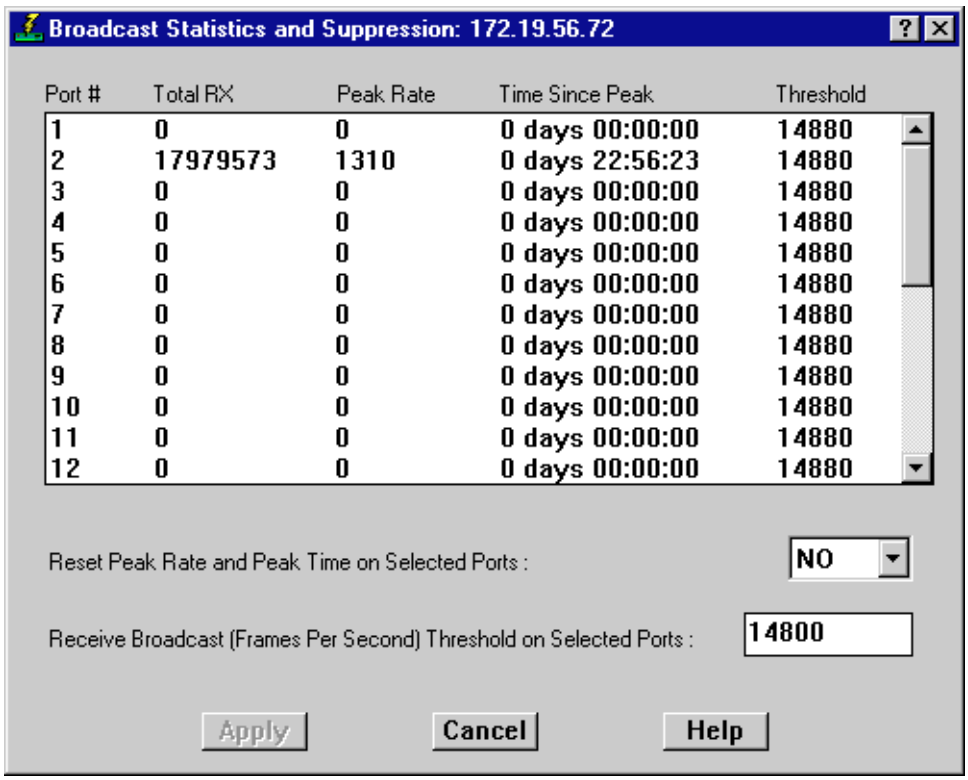


Figure 2-24. The Broadcast Statistics and Suppression Window

Port #
This read-only field indicates the number assigned to each interface on the device.

Total RX
Displays the total number of broadcast frames received on the interface since the device was last initialized.

Peak Rate
The peak rate of broadcast frames (in frames per second) received on the interface since the device was last initialized or the peak value was administratively reset through this window.

Time Since Peak
The time (in a days HH:MM:SS format) since the peak broadcast rate occurred; that is, the current MIB-II system uptime minus the system uptime when the peak occurred (as recorded by the *ctBroadcastPeakBroadcastRateTime* OID). This value will be reset to 0 days 00:00:00 when the device is re-initialized or when you administratively reset the peak values.

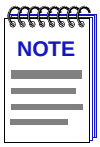
To reset the Peak Rate and Time Since Peak values:

1. Shift- or Control-click to select one or more interfaces for which you want to reset the values.
2. Click on the **Reset Peak Rate and Peak Time on Selected Ports:** drop-down list box, and select **YES**.
3. Click **Apply**. The Peak Rate and Time Since Peak values will be reset for the selected interfaces.

Threshold
The maximum number of received broadcast frames per second that may be forwarded by this interface to other interfaces on the device. Any number of broadcast frames received over this threshold will be dropped. The default value for the interface is near the theoretical maximum frames per second for the interface, i.e., 14,880 for 10Mb Ethernet interface, 148,880 for 100Mb Ethernet or 1,488,800 for Gigabit Ethernet.

To change the Receive Broadcast Threshold:

1. Shift- or Control-click to select one or more interfaces for which you want to change the broadcast packet threshold.
2. Highlight the value currently in the **Receive Broadcast Threshold on Selected Ports:** field and type in a new broadcast threshold value. Allowable values begin at 10 and proceed in multiples of ten**.**



When you enter a value less than 10, the threshold will default to a value of 0. If you enter a value that is not a multiple of 10 it will default to the last multiple of 10, i.e., if you enter 15 as the new threshold value, the threshold value will be set to 10; if you enter 49 as the new threshold value, the threshold value will be set to 40.

3. Click **Apply**. The new threshold will be applied to the selected interfaces. Any broadcast frames received by the interface exceeding the set threshold will be dropped.

The System Resources Window

The System Resources window displays attributes of the MultiSwitch 700 module's CPU (including CPU type, and installed and available memory), as well as the current and peak utilization of the CPU for switching. It also lets you reserve the desired amount of CPU processing used for switching or management purposes, as well as reset the peak switch utilization information.

To display the System Resources window:

1. Click **Device** in the Device View menu bar to display the Device menu.
2. Select **System Resources**. The System Resources window, Figure 2-25, opens.

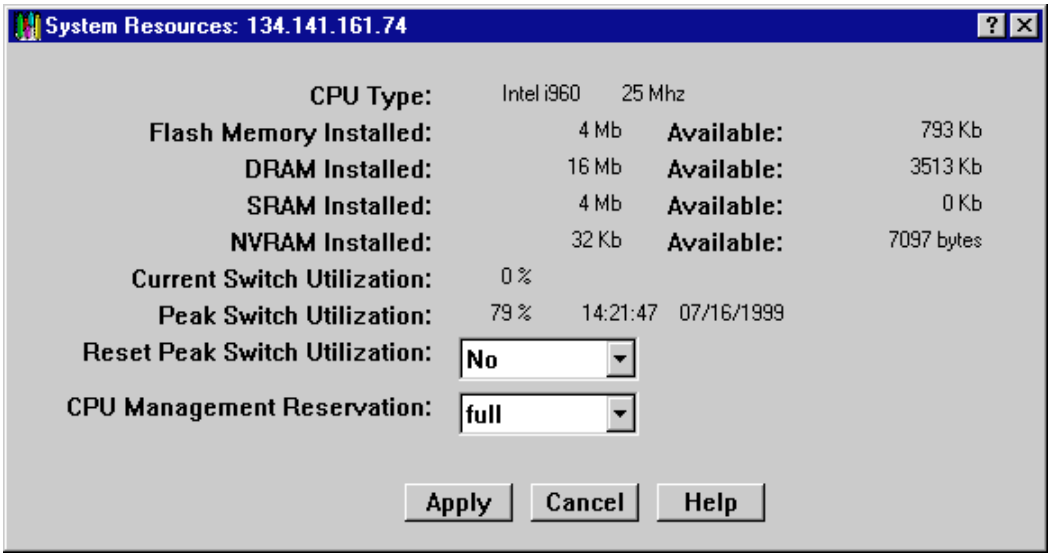


Figure 2-25. The System Resources Window

CPU Type
Displays the type and speed (in megahertz) of the CPU (processor) used by the system.

Flash Memory Installed:
Displays the total amount of installed flash memory (in Mbytes). Flash memory is the reprogrammable memory used to store the device's image code.

Flash Memory Available:
Displays (in Kbytes) the current amount of flash memory that is currently free and not currently being used for code and data.

DRAM Installed:
Displays the total installed Dynamic Random Access Memory (DRAM) in Mbytes. DRAM is volatile memory used to temporarily store data via capacitors and transistors, which must be constantly recharged to retain data. Access time to read data stored on DRAM is slower than reading data stored on Static Random Access Memory (SRAM) — since the processor cannot read DRAM while the capacitors are being recharged. A DRAM chip, however, can store about four times more data than a comparable SRAM chip, and is less expensive to manufacture.

DRAM Available:
Displays (in Kbytes) the amount of free DRAM that is not currently being used for data storage.

SRAM Installed:
Displays the total amount of SRAM (Static Random Access Memory) that is installed (in Mbytes). SRAM retains data as long as the CPU is powered up. Since it does not need the constant recharging of DRAM memory, its data can be accessed much faster. SRAM is often used to temporarily cache — or store — frequently accessed data or instructions commonly used by the processor. SRAM can store less data than DRAM, however, and is more expensive to manufacture.

SRAM Available:
Displays (in Kbytes) the amount of free SRAM that is not currently being used for data storage.

NVRAM Installed:
Displays (in Kbytes) the total installed Non-volatile Random Access Memory (NVRAM). NVRAM retains data when the device is powered down, such as the device IP address, community table information, and so forth.

NVRAM Available:
Displays (in Bytes) the amount of free NVRAM that is not currently being used for data storage.

Current Switch Utilization:
Displays the current load on the switch, which is based on a percentage of maximum switching capacity of 100%.

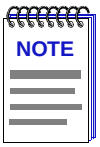
Peak Switch Utilization:
Displays the peak percentage of switch load (based on a maximum of 100%) that has occurred on the switch, since power-up or last reset, along with the time and date that it occurred. This field can be administratively refreshed, as described below.

Reset Peak Switch Utilization:
This option allows you to clear the Peak Switch Utilization field.The Peak Switch Utilization field will refresh to display the current switch utilization, date, and time as the new peak values (until a new peak is experienced).

1. Click on  next to the Reset Peak Switch Utilization field and select **Yes** from the drop down list. (The default value is **No**.)

2. Click **Apply** to reset the displayed peak switch utilization. When the window refreshes the value in this field will return to **No**.

   The peak switch utilization values — including percentage, date, and time — will be refreshed to display the current values. These values will change once a new peak is experienced (or at the next peak reset).



*The default setting for this field is **No**. While **No** is selected the peak switch utilization value will **not** be reset when you click on the **Apply** button. You must choose **Yes** for a reset to take place.*

CPU Management Reservation:
Displays the desired amount of CPU bandwidth reserved for management purposes: None, Limited, or Full. Bandwidth that is not reserved for management will be devoted to switching.

Reserving CPU Bandwidth

Depending on your needs and the main function of your MultiSwitch 700 module, you may wish to change the amount of CPU bandwidth that is currently reserved for management purposes. The three possible allocations of CPU bandwidth on your MultiSwitch 700 for management are:

- **None —** the MultiSwitch 700 will reserve *all* bandwidth for switching, therefore management frames may be dropped under heavy loads.
- **Limited —** the management of the MultiSwitch 700 may be slow while the device is experiencing heavy switching loads.
- **Full —** management of the MultiSwitch 700 is *always* possible and management frames will take priority over switched data if full CPU bandwidth is required (switched frames may be dropped).

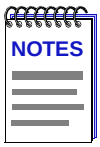
To configure the CPU Management Reservation:

1. Next to the **CPU Management Reservation** field, click on and select **None**, **Full**, or **Limited** from the drop down list.
2. Click on the **Apply** button to set the new CPU management reservation. A window opens stating the set was successful.

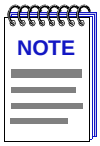
802.1Q VLANs

This section introduces and describes pre-standard IEEE 802.1Q port-based Virtual Local Area Network (VLAN) technology and the windows used to configure 802.1Q VLAN-capable devices.

Current versions of MultiSwitch 700 firmware support the pre-standard IEEE 802.1Q draft specification for port-based VLANs.



For older versions of MultiSwitch 700 firmware, if 802.1Q is to be utilized it is required that all modules in the chassis be configured to operate in 802.1Q mode. Distributed Chassis Management may not be supported for MultiSwitch 700 modules operating in 802.1Q mode. In such cases, it is recommended that all modules installed in the MultiSwitch 700 chassis be configured via Local Management to operate in Standalone mode. Contact the Global Technical Assistance Center for firmware upgrade information.



For current versions of MultiSwitch 700 firmware, DELHF-UA modules cannot be installed in a MultiSwitch 700 that is operating in 802.1Q mode. This will be corrected in a future version of firmware.

What Is A VLAN?

A Virtual Local Area Network (VLAN) is a logical group of devices that function as a single Local Area Network segment (broadcast domain). Devices comprising a VLAN may be (physically) widely separated, allowing users located in separate areas or connected to separate ports to belong to a single VLAN group. Users assigned to a VLAN can send and receive broadcast and multicast traffic as though they were all physically connected to a single network segment. VLAN-capable switches isolate broadcast and multicast traffic received from VLAN groups, and contain broadcasts and multicasts from members of a VLAN within that group.

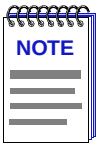
What Is An 802.1Q Port-Based VLAN?

Switches that support the pre-standard IEEE 802.1Q draft specification for port-based VLANs act by classifying frames into VLAN membership. Usually, VLAN classification is based on tag headers (VLAN tags) in the headers of data frames. The tag header is inserted into the frame directly after the Source MAC address field. A four-byte field in the tag header is used as the VLAN identifier. These VLAN tags are added to data frames by the switch as the frames are transmitted and / or received by certain ports, and are later used to make forwarding decisions by the switch and other 802.1Q switches. In the absence of a VLAN tag, a frame is assigned VLAN membership according to the VLAN configuration of the switch port that receives the frame.

About 802.1Q VLAN Configuration and Operation

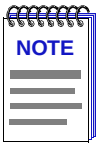
An 802.1Q VLAN is defined by assigning it a unique identification number (the VLAN ID) and an optional name. The VLAN ID is used to identify data frames that originate from, and are intended for, the ports assigned to the VLAN. Up to 64 VLANs may be created, with VLAN IDs ranging from 2-4094. VLAN ID 1 is reserved for the Default VLAN.

Ports on 802.1Q switches are assigned membership in a VLAN by associating a VLAN ID with each port on the switch. The VLAN ID is combined with the port's identification (e.g., module X port X) to form the Port VLAN ID (PVID).



When 802.1Q mode is initially activated on a device, all ports are associated with the Default VLAN (VLAN ID 1). If a VLAN ID has ***not*** *been assigned to a particular port on an 802.1Q switch, any frames received from that port will be classified as belonging to the Default VLAN.*

When 802.1Q is implemented for a MultiSwitch 700 that has a DELHA-UA installed, each LEC will be represented as an individual port which can be easily assigned membership in a VLAN.



For current versions of MultiSwitch 700 firmware, the number of LECs supported by the DELHA-UA in 802.1Q mode is limited to 32.

Once VLANs have been configured and activated, all frames with unknown destination addresses (including broadcast, unknown multicast, and unknown unicast frames) will be contained within the VLAN of their origin. The switch's Filtering Database tracks the associations between MAC addresses, VLAN eligibilities, and port numbers, and is used to make forwarding decisions for frames. All VLANs share a single Spanning Tree.

Ingress List Operation

A port's ingress list specifies the VLAN with which received frames will be associated. The switch's Filtering Database tracks the associations between VLAN eligibilities, MAC addresses, and port numbers.

Untagged frames received by an 802.1Q switch port are classified according to the VLAN membership of the port that receives the frame.

Tagged frames received by an 802.1Q switch port are classified according to the VLAN indicated in their tag header. A port may receive a tagged frame that specifies a VLAN other than the one assigned to the port.

Egress List Operation

Each port's egress list specifies which VLANs are associated with the port, and specifies what type of frame (tagged or untagged) to transmit for each particular VLAN on a port. This information may be statically defined by the user, or dynamically learned and maintained by the switch's Filtering Database.

If a port receives a tagged frame that specifies a VLAN other than the one assigned to the port, the switch will dynamically associate that frame's source address and VLAN with the port (i.e., add that frame's VLAN to the receiving port's egress list). Dynamically learned VLANs are subject to the same aging rules as source addresses (e.g., if a tagged frame belonging to a dynamically learned VLAN is not received by the port within the switch's aging time, the transmitting station's source address and VLAN will be aged out for that port; no unknown destination frames belonging to the station's VLAN will be transmitted through the port until the VLAN is dynamically learned once again). Only tagged frames can cause the switch to dynamically change a port's egress list.

802.1Q Port Types

Each 802.1Q switch port is assigned a mode of operation. Port types include:

1Q Trunk

If VLAN membership is to apply to users across several switches, ports used to connect 802.1Q-aware devices are configured to use 1Q Trunk mode. In this mode, all frames (except BPDUs) are transmitted with a tag header included in the frame, allowing VLAN frames to maintain their VLAN ID across multiple switches. Any untagged frames received by the port are dropped. 1Q Trunk ports are configured to be members of all VLANs.

1d Trunk

This mode allows a port to transmit to a traditional (802.1d) switch fabric. These ports transmit only untagged frames, and the switch expects to receive only untagged traffic through the port. 1d Trunk ports are configured to be members of all VLANs. This mode can be used to share a connection among multiple VLANs (e.g., sharing a server between two or more separate VLANs).

Hybrid

Hybrid mode (enabled by default) allows a port to receive and transmit both tagged and untagged frames. In this mode, the port will be a member of its statically assigned VLAN, as well as any dynamically learned VLANs (remember, dynamically learned VLANs are subject to the same aging rules as source addresses).

Configuring Your 802.1Q VLANS

Before you can define and configure 802.1Q port-based VLANs on your device, you must activate the device's 802.1Q operational mode; this operation can be performed using Local Management or the Mib Tools application. Using Mib Tools, 802.1Q mode can be activated through the Container Mib's Logical Entry Table (*contLogicalEntryTable*). When the 802.1Q component is activated, the device will automatically reset, and begin operating in 802.1Q mode.

For older versions of MultiSwitch 700 firmware, if 802.1Q is to be utilized it may be required that all modules in the chassis be configured to operate in 802.1Q mode. If you attempt to activate a MultiSwitch 700 module's 802.1Q component via the Mib Tools application, you may lose contact with the rest of the chassis once the device resets. For this reason, we recommend that Local Management be used to activate 802.1Q mode for MultiSwitch 700 modules.

Refer to your device's Local Management documentation for instructions on activating a device's 802.1Q operational mode via Local Management. For details on the Mib Tools application, refer to your ***Tools Guide***.

To set up your 802.1Q port-based VLANs using NetSight Element Manager, you must first define the desired VLANs using the VLAN Config window (Figure 2-26), which allows you to assign VLAN IDs and optional VLAN names, and enable or disable VLANs.

After your VLANs are defined, you may configure the ingress and egress lists for each port using the VLAN Port Config window (Figure 2-27) and the VLAN Egress Port Config window (Figure 2-28), respectively.

Setting VLAN Parameters and Operational Modes

802.1Q VLANs are defined using the VLAN Config window, which is accessed from the **Device** menu in your switch's Device View. To launch the window:

1. Click on **Device** in the Device View menu bar to display the Device menu.
2. Click on **802.1Q VLAN** and then right to select **802.1Q VLAN Config**. The VLAN Config window, Figure 2-26, opens.

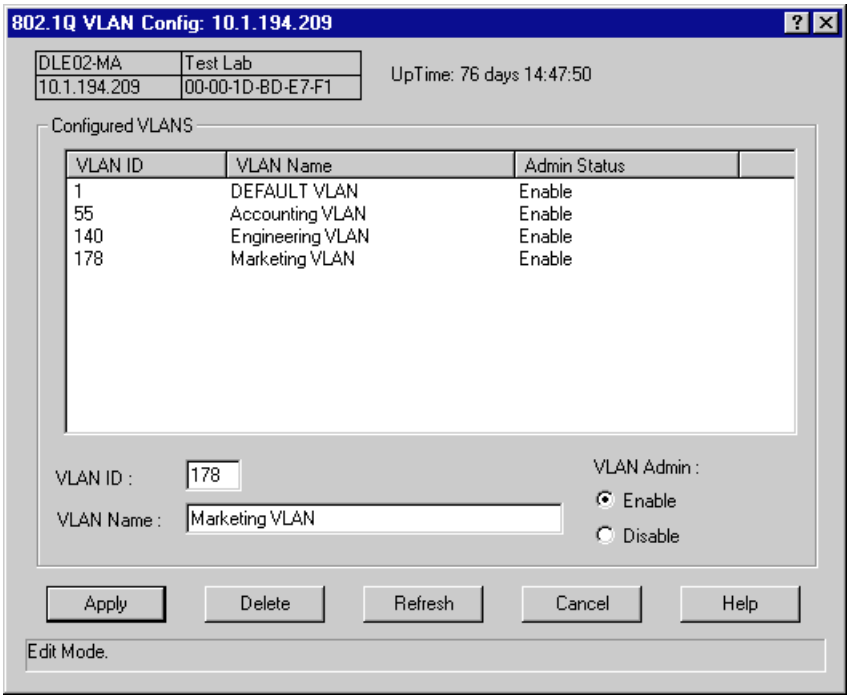


Figure 2-26. The VLAN Config Window

The **Configured VLANS** list box and fields allow you to view, create, modify, delete, enable, and disable 802.1Q port-based VLANs. The list box displays the following information about your defined VLANs:

VLAN ID

The VLAN ID is used to identify data frames that originate from, and are intended for, the ports assigned to the VLAN. Up to 64 VLANs may be created, with VLAN IDs ranging from 2-4094. The VLAN ID is combined with the port's identification (e.g., module X port X) to form the Port VLAN ID (PVID). VLAN ID **1** is reserved for the Default VLAN.

VLAN Name

An optional 32-character VLAN name may be assigned to a created VLAN. The Default VLAN is assigned the name **DEFAULT VLAN**, which cannot be changed or deleted.

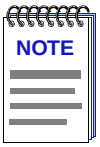
Admin Status

This field indicates whether the VLAN is enabled or disabled. Unless **Enable** is selected when port-based VLANs are initially defined, they are disabled by default. The Default VLAN cannot be disabled.

Creating and Modifying VLANs

The fields immediately below the **Configured VLANS** list box are used to create and modify your port-based VLANs. To create a new VLAN:

1. In the **VLAN ID** field, enter a unique value between **2**-**4094**. VLAN ID **1** is reserved for the Default VLAN, and cannot be used.
2. If desired, enter a name for the VLAN in the **VLAN Name** field. VLAN names must be 32 characters or less.



*Unless **Enable** is selected when a port-based VLAN is initially defined, it will be disabled by default. A new VLAN that is left in a **Disabled** state will remain disabled until a port is assigned to it, at which time it will be automatically enabled. If you are changing a VLAN's port assignment, the VLAN should be disabled before changing the port configuration. See **Enabling and Disabling VLANs**, on page 2-67, for instructions on disabling VLANs. See **Performing Ingress List Configuration**, on page 2-67, for details on completing your VLAN port configuration.*

3. Click the **Apply** button. The new VLAN will be added to the **Configured VLANS** list box.

Once a VLAN has been created, its VLAN ID cannot be modified. If you wish to change a VLAN's ID, you'll have to delete the VLAN and create a new entry. See **Deleting VLANs**, below, for instructions on deleting a VLAN. Attempting to change a VLAN's ID will result in the creation of a new VLAN with the same VLAN name.

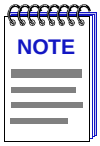
To modify an existing VLAN's name, select its entry in the **Configured VLANS** list box. The selected VLAN's name will be displayed in the **VLAN Name** field. Modify the displayed name as outlined in Steps 2-3, above.

Deleting VLANs

The VLAN Config window also allows you to delete VLANs (except for the Default VLAN, which cannot be deleted). When a VLAN is deleted, any ports assigned to that VLAN will automatically become members of the Default VLAN. To delete a VLAN from your 802.1Q switch:

1. Click to select the desired VLAN entry in the **Configured VLANS** list box.
2. Click the **Delete** button. The selected VLAN will be removed from the list box.

Enabling and Disabling VLANs



*Unless **Enable** is selected when a VLAN is initially defined, it is disabled by default. A new VLAN that is left in a **Disabled** state will remain disabled until a port is assigned to it, at which time it will be automatically enabled. If you are changing a VLAN's port assignment, the VLAN should be disabled before changing the port configuration. See **Performing Ingress List Configuration**, on page 2-67, for details on completing your VLAN port configuration.*

To enable or disable VLANs:

1. Select the desired VLAN entry in the **Configured VLANS** list box.
2. In the **VLAN Admin** field, click to select **Enable** or **Disable**.
3. Click the **Apply** button. The selected VLAN will be enabled or disabled, depending on your selection.

Updating VLAN Config Window Information

Clicking the **Refresh** button will update the information displayed in the Configured VLANs list without closing the window.

Performing Ingress List Configuration

802.1Q VLAN port assignment and ingress list configuration operations are performed using the VLAN Port Config window, which is accessed from the **Device** menu in your switch's Device View. See **Ingress List Operation**, on page 2-62 for details on ingress lists. To launch the window:

1. Click on **Device** in the Device View menu bar to display the Device menu.
2. Click on **802.1Q VLAN** and then right to select **802.1Q VLAN Port Config**. The VLAN Port Config window, Figure 2-27, opens.

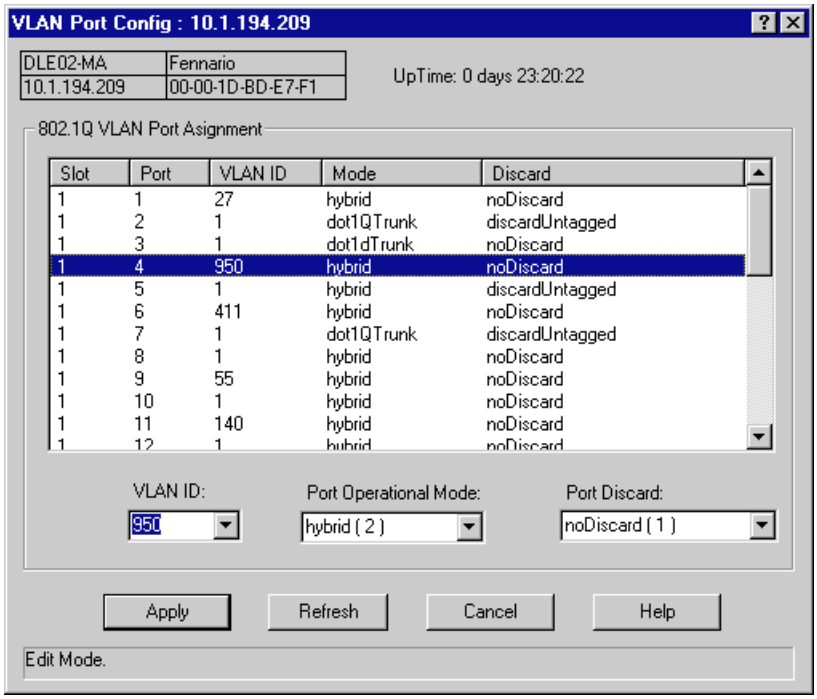


Figure 2-27. The VLAN Port Config Window

The **802.1Q VLAN Port Assignment** list box in this window displays the following information about ports on your 802.1Q switch:

Slot/Port

These fields display the slot and port index for each port on your 802.1Q switch.

VLAN ID

This field displays the VLAN ID of the VLAN to which the port is currently assigned.

Mode

This field displays the port's current mode of operation. Port operational modes include:

- **Dot1DTrunk** mode, which is used for ports that are to connect to a traditional (802.1D) switch fabric. These ports transmit only untagged frames. 1d Trunk ports are configured to be members of all VLANs.
- **Dot1QTrunk** mode, which is used for ports used to connect 802.1Q-aware devices if VLAN membership is to apply to users across several switches. These ports transmit only tagged frames. 1Q Trunk ports are configured to be members of all VLANs.

- **Hybrid** mode, which allows a port to receive and transmit both tagged and untagged frames. In this mode, the port will be a member of its statically assigned VLAN, as well as any dynamically learned VLANs. Hybrid mode is enabled by default.

For more information on 802.1Q port operational modes, see **802.1Q Port Types**, on page 2-63.

Discard

This field displays the port's current frame discard format (**discardTagged**, **discardUntagged**, or **noDiscard**).

The **VLAN ID**, **Port Operational Mode**, and **Port Discard** fields, below the list box, allow you to configure your ports as follows:

VLAN ID

This field allows you to associate a selected port with an existing VLAN. See **Assigning VLAN Membership to Ports**, on page 2-69, for details on performing this operation.

Port Operational Mode

This field allows you to assign a mode of operation to a selected port. See **Setting Port Operational Modes**, on page 2-70, for details on using this field.

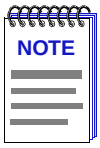
Port Discard

This field allows you to specify the frame discard format (discardTagged, discardUntagged, or noDiscard) for a selected port. See **Setting Port Frame Discard Formats**, on page 2-70, for details on using this field.

Assigning VLAN Membership to Ports

To assign a port on your 802.1Q switch to any of your defined VLANs:

1. In the list box, click to select a port that you wish to assign to a VLAN. The port's current VLAN configuration information, including its VLAN ID, will be displayed in the fields below the list box.
2. In the **VLAN ID** field, click to select the VLAN ID of the VLAN to which you wish to assign the selected port.
3. Click the **Apply** button. The new VLAN assignment will be reflected in the VLAN Port Config window's list box for the selected port.



*If you assign a port to a VLAN that is in a **Disabled** state, the VLAN will automatically be **Enabled** once the port assignment operation has been completed.*

Setting Port Operational Modes

To assign a port operational mode (**dot1dTrunk**, **dot1QTrunk**, or **hybrid**) to a port on your 802.1Q switch:

1. In the VLAN Port Config window's list box, click to select a port to which you wish to assign a port operational mode.
2. In the **Port Operational Mode** field, click to select the desired operational mode.
3. Click the **Apply** button. The selected mode will be reflected in the list box for the selected port.

Setting Port Frame Discard Formats

To assign a frame discard format (**discardTagged**, **discardUntagged**, or **noDiscard**) to a port on your 802.1Q switch:

1. In the VLAN Port Config window's list box, click to select a port to which you wish to assign a frame discard format.
2. In the **Port Discard** field, click to select the desired frame discard format.
3. Click the **Apply** button. The selected mode will be reflected in the list box for the selected port.

Updating VLAN Port Config Window Information

Clicking the **Refresh** button will update the information displayed in the 802.1Q VLAN Port Assignment list without closing the window.

Performing Egress List Configuration

802.1Q VLAN switching allows each port on a switch to transmit traffic for any or all defined VLANs on your network. During egress list configuration, you determine which VLANs are on each port's egress list. See **Egress List Operation**, on page 2-62 for details on egress lists.

Egress list configuration operations are performed using the VLAN Egress Port Config window. To launch the window:

1. Click on **Device** in the Device View menu bar to display the Device menu.
2. Click on **802.1Q VLAN** and then right to select **802.1Q VLAN Egress Port Config**. The VLAN Egress Port Config window, Figure 2-28, opens.

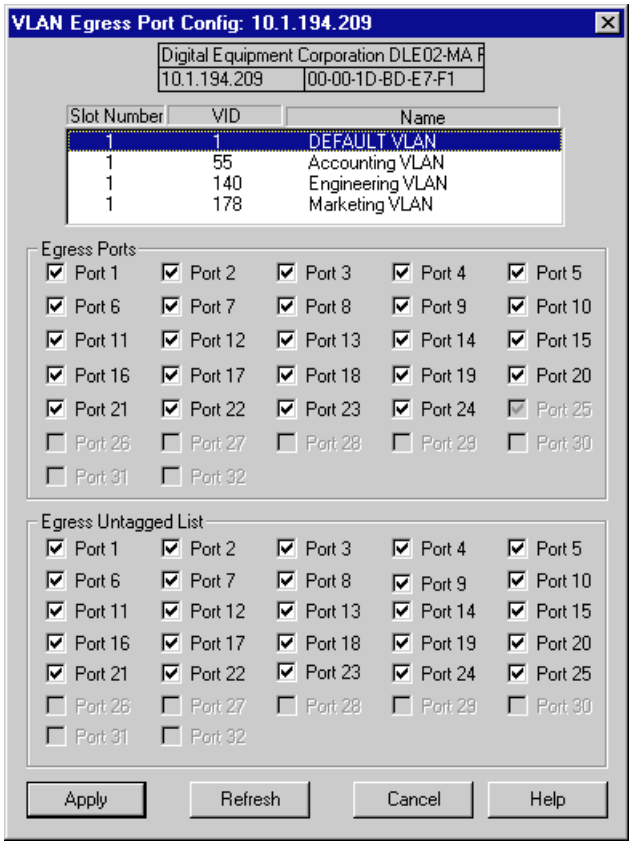


Figure 2-28. The VLAN Egress Port Config Window

The list box at the top of this window is used to select a configured VLAN for association with your switch's ports. Clicking on a VLAN will display its currently associated ports in the lower portion of this window. The list box displays the following information:

Slot Number
This field displays the slot index for the module being configured.

VID
This field lists the VLAN IDs of the currently configured VLANs on your switch.

Name
This field lists the VLAN names assigned to the currently configured VLANs on your switch.

Under the list box there are two groups of check boxes that display the ports on the switch. A checkmark in the port's check box indicates that the VLAN selected in the list box is in the port's egress list. The two groups are:

Egress Ports
Use these check boxes to add or remove the selected VLAN from the egress list of one or more ports.

Egress Untagged List
Use these check boxes to allow the ports to transmit untagged frames from the selected VLAN.

Building an Egress List

To build egress lists for your 802.1Q switch:

1. In the list box at the top of the window, click to select a configured VLAN. The ports that contain the selected VLAN in their egress lists will be displayed in the lower portions of this window with checkmarks in their check boxes.
2. To add or remove the selected VLAN from the egress list of one or more ports, click on the appropriate check box in the **Egress Ports** group. A checkmark in a port's check box indicates that the selected VLAN is in the port's egress list.
3. To add or remove the ability for a port to transmit both tagged and untagged frames from the selected VLAN, click to put a checkmark in the appropriate check box in the **Egress Untagged List** group. Note that a port check box in this group will be grayed out until it has been selected in the Egress Ports group.
4. To apply any changes, click on the **Apply** button at the bottom of the window.

Setting the Device Date and Time

The **Device** menu provides the options that allow you to change the date and time stored in the device's internal clock: **Edit Device Time** and **Edit Device Date**.

To edit the device time:

1. Click on **Device** on the Device View menu bar to access the Device menu.
2. Select **Edit Device Time**. The Device Time change window, Figure 2-29, opens.

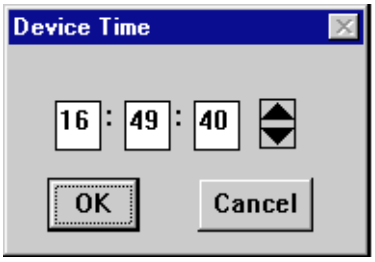


Figure 2-29. The Device Time Window

3. Enter the new time in a 24-hour hh:mm:ss format, either by highlighting the field you wish to change and using the up and down arrow buttons, or by entering the new value in the appropriate field.
4. Click **OK** to save your changes, or **Cancel** to exit without saving changes.

To edit the device date:

1. Click on **Device** on the Device View menu bar to access the Device menu.
1. Select **Edit Device Date**. The Device Date change window, Figure 2-30, opens.

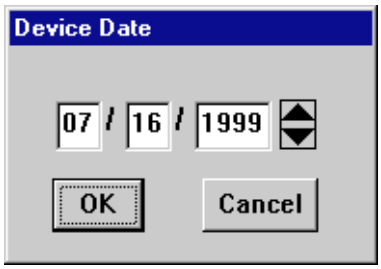
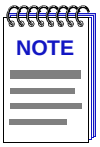


Figure 2-30. The Device Date Window

2. Enter the new date in a mm/dd/yyyy format, either by highlighting the field you wish to change and using the up and down arrow buttons, or by entering the new value in the appropriate field.
3. Click **OK** to save your changes, or **Cancel** to exit without saving changes.

Enabling and Disabling Ports

When you disable bridging at a port interface, you disconnect that port's network from the bridge entirely. The port does not forward any packets, nor does it participate in Spanning Tree operations. Nodes connected to the network can still communicate with each other, but they can't communicate with the bridge or with other networks connected to the bridge. When you enable bridging for the interface, the port moves from the Disabled state through the Listening and Learning states to the Forwarding state; bridge port state color codes will change accordingly.



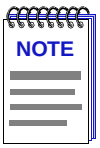
You cannot disable a backplane interface from the Device Logical View — since the backplane interfaces do not appear in the port stack. You must use the Device BackPlane Config View to disable the interfaces to the DLM6C-AA backplane.

To enable or disable bridging for an individual interface:

1. Click on the appropriate port display box to display the port menu.
2. Select **Enable** to enable bridging at the interface, or **Disable** to disable bridging. Bridging will now be enabled or disabled across the selected port, as desired.

To enable or disable bridging for all interfaces installed on the monitored MultiSwitch 700 module:

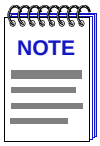
1. Click on the **module index** of interest to display the Module menu.
2. Select **Enable Bridge** to enable bridging at all installed interfaces, or **Disable Bridge** to disable bridging across all interfaces. Bridging will now be enabled or disabled across the installed interfaces, as desired.



For more information about bridging functions and how to determine the current state of each bridge port, see the ***Bridging*** *chapter in the* **Tools Guide**.

The DELHW-UA Device View

Unlike other modular interfaces designed for the MultiSwitch 700 boards, the DELHW-UA module functions as an independent intelligent device with its own IP address. As such, it must be managed separately from the MultiSwitch 700 chassis and the board on which it is installed. This section provides information on launching the DELHW-UA Device View and using its associated functions. For information on configuring and managing the WAN capabilities of the various port modules available for the DELHW-UA, see **Chapter 7**.



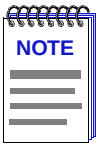
QuickSET for the DELHW-UA was shipped with your device. This program is designed for point-and-click installation and set-up of DELHW-UA devices. If you launch Chassis Manager for a DELHW-UA and have QuickSET installed, your Utilities menu will display a menu pick for launching QuickSET. See your QuickSET for the DELHW-UA documentation for more information.

Port interface modules available for the DELHW-UA include:

DELDS-UI	DDS is Digital Data Services, a digital network that supports data rates of 56Kbps or 64Kbps. The DDS service provides users with dedicated, two-way simultaneous transmission capabilities operating at transfer rates up to 64 Kbps. This port module comes with a built-in CSU / DSU.
DELDI-UI	The DI (Drop-and-Insert) port interface module provides a T1 interface through a front-panel RJ45 port and includes a built-in CSU / DSU for direct connection to a T1 line. The DELDI-UI provides Full T1 or Fractional T1 using 56 or 64 Kbps Time Slots. It also provides a second Drop-and-Insert interface that allows more than one device, such as a PBX, to share a single T1 connection.
DELE1-UI	This port interface module provides an E1 interface through a front-panel RJ-45 port and includes a built-in CSU / DSU for direct connection to an E1 line. It provides Full E1 or Fractional E1 using 56 or 64 Kbps Time Slots with a total throughput of up to 2 Mbps. Time Division Multiplexing (TDM) allows for the channelization of up to 31 links of a single physical interface.

DELST-UI	This port interface module provides an ISDN 128 Kbps Basic Rate Interface (BRI) and is designed for an ISDN back-up link for a frame relay or leased line. In the United States and Canada, Network Terminator equipment (NT1) is required to provide an interface between the DELST-UI and the ISDN line.
DELSY-UI	Provides a synchronous serial connection of up to 2.048 Mbps to external communications equipment (an external CSU / DSU is required). An external CSU / DSU is required; the following electrical interfaces are supported (consult your hardware documentation for cable pinout information): EIA-RS449 V.35 EIA-RS232D X.21 EIA-RS530 EIA-530A RS530 ALT A RS530A ALT A
DELT1-UI	Provides a T1 interface through a front-panel RJ45 port and includes a built-in CSU / DSU for direct connection to a T1 line. The DELT1-UI provides both Full T1 or Fractional T1 using 56 or 64 Kbps Time Slots, with a total throughput of up to 1.544 Mbps. Time Division Multiplexing (TDM) allows for channelization of up to 24 links over a single physical T1 / FT1 interface.
DELTD-UI	This port interface module provides both a T1 and DDS interface that allows you to easily switch between the two interfaces by changing the physical cabling and reconfiguring the desired interface with either QuickSET for the DELHW-UA or NetSight Element Manager.

For more information on these port modules, consult the appropriate hardware documentation or your QuickSET for the DELHW-UA documentation.



To configure the DELDI-UI and DELE1-UI, use the QuickSET application that was shipped with your device. See your QuickSET for the DELHW-UA documentation for more information.

Launching the DELHW-UA Device View Window

The DELHW-UA Device View window is the main screen that immediately informs you of the current condition of individual ports on your switch via a graphical display. The Device View window also serves as a single point of access to all other DELHW-UA windows and screens, which are discussed throughout this manual.

To access the DELHW-UA Device View window, use one of the following options:

1. In any map, list, or tree view, double-click on the DELHW-UA you wish to manage.

   or

1. In any map, list, or tree view, select the DELHW-UA you wish to manage.
2. Select **Manage—>Node** from the primary window menu bar, or select the Manage Node  toolbar button.

   or

1. In any map, list, or tree view, click the **right** mouse button once to select the DELHW-UA you wish to manage and on the resulting menu, select **Manage**.

Viewing Device Information

The desired DELHW-UA Device View window (Figure 2-31) provides a graphical representation of the device, including a color-coded port display which immediately informs you of the current configuration and status of the switch and its ports.

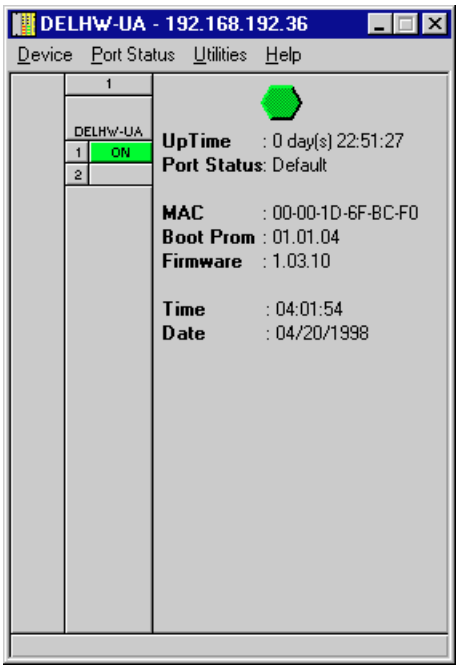


Figure 2-31. The DELHW-UA Device View Window

NOTES

The Device View windows will only display the bridge ports on a DELHW-UA. See your QuickSET for the DELHW-UA documentation for information on managing your Ethernet ports.

By clicking in designated areas of the chassis graphical display (as detailed later in this chapter), or by using the menu bar at the top of the Device View window, you can access all of the menus that lead to more detailed device- and port-level windows.

TIP

When you move the mouse cursor over a management "hot spot" the cursor icon will change into a "hand" to indicate that clicking in the current location will bring up a management option.

Front Panel Information

The areas surrounding the main chassis area provide the following device information:

IP

The Internet Protocol address assigned to the DELHW-UA appears in the title bar of the Device View window. IP addresses are assigned via Local Management.

Connection Status 

This color-coded area indicates the current state of communication between NetSight Element Manager and the DELHW-UA.

- **Green** indicates the DELHW-UA is responding to device polls (valid connection).
- **Magenta** indicates that the DELHW-UA is in a temporary stand-by mode while it responds to a physical change in the switch; note that board and port menus are inactive during this stand-by state.
- **Blue** indicates an unknown contact status — polling has not yet been established with the DELHW-UA.
- **Red** indicates the DELHW-UA is not responding to device polls (device is off line, or device polling has failed across the network for some other reason).

UpTime

The amount of time, in a X day(s) hh:mm:ss format, that the DELHW-UA has been running since the last start-up.

Port Status

If management for your device supports a variable port display (detailed in **The DELHW-UA Port Status Displays**, on page 2-83), this field will show the display currently in effect. If only a single port display is available — or if the default view is in effect — this field will state **Default**.

MAC

Displays the physical layer address assigned to the interface associated with the IP Address used to define the device icon when it was added to NetSight Element Manager. MAC addresses are hard-coded in the device, and are not configurable.

Boot Prom

The revision of BOOT PROM installed in the DELHW-UA.

Firmware

The revision of device firmware stored in the DELHW-UA's FLASH PROMs.

Time

The current time, in a 24-hour hh:mm:ss format, set in the DELHW-UA's internal clock.

Date

The current date, in an mm / dd / yyyy format, set in the DELHW-UA's internal clock.

Menu Structure

By clicking on various areas of the DELHW-UA Device View display, you can access menus with device- and port-level options, as well as utility applications which apply to the device. The following illustration displays the menu structure and indicates how to use the mouse to access the various menus:

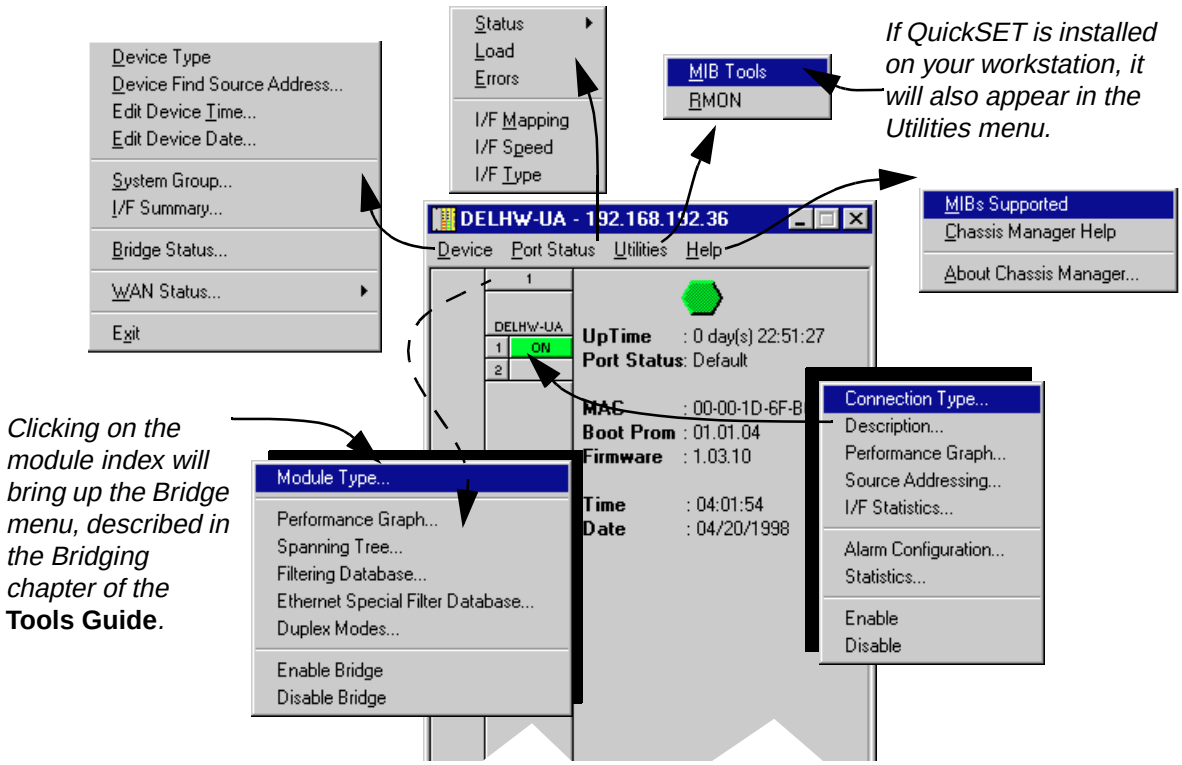


Figure 2-32. DELHW-UA Device View Menu Structure

The Device Menu

From the Device Menu at the Device View window menu bar, you can access the following selections:

- **Device Type** displays a description of the device being modeled. See **Viewing Hardware Types**, on page 2-20.
- **Device Find Source Address** allows you to conduct a search to discover which interface(s) a specified source MAC address is communicating through. See **Viewing I/F Summary Information**, on page 2-22.

- **Edit Device Time / Edit Device Date** allows you set the device's internal clock. See **Setting the Device Date and Time**, on page 2-72.
- **System Group** allows you to manage the DELHW-UA via SNMP MIB II. Refer to the ***Generic SNMP Guide*** for further information.
- **I/F Summary** allows you to view statistics (displayed both graphically and numerically) for the traffic processed by each network interface on your DELHW-UA. See **Viewing I/F Summary Information** on page 2-22 for more information.
- **Bridge Status** provides an overview of bridging information for each interface, and allows you to access all other bridge-related options. Refer to the Bridging chapter in the ***Tools Guide*** for more information.
- **WAN Status** accesses the WAN Logical View window of your device. See Chapter 7, **WAN Configuration**, for more information.
- **Exit** closes the DELHW-UA Device View window.

The Port Status Menu

The Port Status Menu allows you to select the status information that will be displayed in the port text boxes in the Device View window:

- **Status** allows you to select one of four status type displays: Bridge, Bridge Mapping, Admin, or Operator.
- **Load** allows you to display the portion of network load processed per polling interval by each interface as a percentage of the theoretical maximum load (10 or 100 Mbps).
- **Errors** allows you to display the number of errors detected per polling interval by each interface as a percentage of the total number of valid packets processed by the interface.
- **I/F Mapping** will display the interface *ifIndex* associated with each port on your DELHW-UA.
- **I/F Speed** will display the speed (10 or 100 Mbps) of the network segment attached to each port. The speed of the network management port will be displayed in Kbps.
- **I/F Type** will display the interface type of each port in the DELHW-UA — i.e., Eth (ethernet-csmacd) for the bridging interfaces, and PPP for the network management port.

For more information on the port display options available via this menu, see **The DELHW-UA Port Status Displays**, on page 2-83.

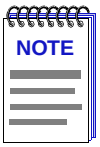
The Utilities Menu

From the **Utilities** menu you can select the following options:

- **MIB Tools**, which provides direct access to the DELHW-UA's MIB information.

- **RMON**, for launching the Remote Network Monitoring application. RMON is described in its the ***Remote Monitoring (RMON) User's Guide***.

These selections are also available from the **Tools** menu at the top of NetSight Element Manager's main window.



You will be able to launch the QuickSET for the DELHW-UA application from the Utilities menu, provided it is installed on your machine. See your QuickSET for the DELHW-UA documentation for more information.

The Help Menu

The Help Menu has the following three selections:

- **MIBs Supported** brings up the Chassis Manager window, described in **The Chassis Manager Window** on page 2-18.
- **Chassis Manager Help** brings up a help window with information specifically related to using the Chassis Manager and Device View windows.
- **About Chassis Manager** brings up a version window for the Chassis Manager application in use.

The Port Menus

The menu for bridging ports offers the following selections:

- **Connection Type** opens a window displaying a description of the connection type of the selected bridge interface. This description is comprised of text based on the *ctIfConnectionType* MIB. See **Connection Type**, on page 2-21 for details.
- **Description** brings up a window describing the selected port; see **Interface Description**, on page 2-21.
- **Performance Graph** allows you to view the traffic going through a selected bridge. This information is displayed both numerically and graphically, as described in the **Bridging** chapter of the ***Tools Guide***.
- **Source Addressing** displays a list of MAC Addresses that communicate through the selected bridge port.
- **I/F Statistics** launches a window that displays MIB-II interface statistics for the selected interface. See Chapter 3, **Statistics**, for more information.
- **Alarm Configuration** launches the RMON-based Basic and Advanced Alarm applications; see Chapter 4, **Alarm Configuration**, for details.

- **Statistics** launches the highest level of statistics currently available for the selected port. For standard Ethernet and Fast Ethernet ports, RMON statistics will be displayed if the RMON Default MIB component is active; if it has been disabled, MIB-II interface statistics will display. See Chapter 3, **Statistics**, for more information.
- **Enable/Disable** administratively turns the selected bridging port on or off; see **Enabling and Disabling Ports** on page 2-85 for more information.

The DELHW-UA Port Status Displays

When you open the Device View window, each port on the DELHW-UA will display its Admin status (defined below). To change this status display, select one of the options on the Port Status menu, as described in the following sections.

To change the status of your ports:

1. Click on **Port Status** on the menu bar at the top of the Device View window; a menu displays.
2. Drag down (and to the right, if necessary) to select the status information you want to display. The port text boxes will display the appropriate status information.

Port status view options are:

Status

You can view four port **Status** categories, as follows:

- **Bridge** — FWD, DIS, LRN, LIS, BLK, BRK, or UNK
- **Bridge Mapping** — bridge interface index numbers
- **Admin** — ON or OFF
- **Operator** — ON or OFF

If you have selected the **Bridge** status mode, a port is considered:

- FWD (Forwarding) if the port is on-line and forwarding packets across the DELHW-UA from one network segment to another.
- DIS (Disabled) if bridging at the port has been disabled by management; no traffic can be received or forwarded on this port, including configuration information for the bridged topology.
- LRN (Learning) if the Forwarding database is being created, or the Spanning Tree Algorithm is being executed because of a network topology change. The port is monitoring network traffic, and learning network addresses.
- LIS (Listening) if the port is not adding information to the filtering database. It is monitoring Bridge Protocol Data Unit (BPDU) traffic while preparing to move to the forwarding state.

- BLK (Blocking) if the port is on-line, but filtering traffic from going across the DELHW-UA from one network segment to another. Bridge topology information will be forwarded by the port.
- BRK (Broken) if the physical interface has malfunctioned.
- UNK (Unknown) if the interface's status cannot be determined.

If you have selected **Bridge Mapping**, the port status boxes will display the *bridge* interface index numbers assigned to each interface (which may or may not match the *ifIndex* values displayed via the **I/F Mapping** option described on page 2-84).

If you have selected the **Admin** status mode, a port is considered:

- ON if the port is enabled by management and has a valid link.
- OFF if it has not been enabled or if it has been disabled through management action.

If you have selected the **Operator** status mode, a port is considered:

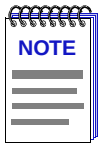
- ON if the port is currently forwarding packets.
- OFF if the port is not currently forwarding packets.

Load

If you choose **Load**, the interface text boxes will display the percentage of network load processed by each port during the last polling interval. This percentage reflects the network load generated per polling interval by devices connected to the port compared to the theoretical maximum load (10 or 100 Mbps) of an Ethernet network.

Errors

If you choose the **Errors** mode, the interface boxes will display the percentage of the total number of valid packets processed by each port during the last polling interval that were error packets. This percentage reflects the number of errors generated during the last polling interval by devices connected to that port compared to the total number of valid packets processed by the port.



The polling interval is set using the Device Management page of the Options window, accessed via the ***Tools —> Options*** *selection from the main menu bar. Refer to the* **User's Guide** *for information on setting node polling intervals.*

I/F Mapping

If you choose the **I/F Mapping** mode, the interface boxes will display the interface number (*IfIndex*) associated with each port on the DELHW-UA.

I/F Speed

If you choose the **I/F Speed** mode, the port text boxes will display the speed of the network segment connected to each port. The speed of the network management port will be displayed in Kbps.

I/F Type

If you choose the **I/F Type** mode, the interface boxes will display the interface type of each port on the DELHW-UA (e.g., Eth, PPP, other).

Port Status Color Codes

The Port Status display options — Bridge, Admin, and Operator — incorporate color coding schemes. For the Admin and Operator **Status** display options, green = ON, red = OFF, and blue = N/A (not available). For the Bridge **Status** display option, green = forwarding, blue = disabled, magenta = learning and listening, orange = blocking, red = broken, and gray = unknown.

For all other Port Status selections — Load, Errors, I/F Port Mapping, Speed, and Type — color codes will continue to reflect the most recently selected mode which incorporates its own color coding scheme.

Managing the Device

The Device View provides you with the basic tools available to configure your device and keep it operating properly.

Enabling and Disabling Ports

From the Port menus on the DELHW-UA Device View window, you can administratively enable and disable the ports.

When you administratively disable a bridge port, you disconnect that port's network from the bridge entirely. The port does not forward any packets, nor does it participate in Spanning Tree operations. Nodes connected to the network can still communicate with each other, but they can't communicate with the bridge or with other networks connected to the bridge. When you enable a port, the port moves from the Disabled state, through the Learning and Listening states, to the Forwarding state; bridge port state color codes will change accordingly.

To enable or disable a bridge port:

1. Click on the desired Port index. The Port menu displays.
2. Click on **Enable** to enable the port, or **Disable** to disable the port. Your port will now be enabled or disabled as desired.

Chapter 3

Statistics

Accessing interface statistics from the Device View; available statistics windows

Each port menu in the Device Logical View window provides two statistics selections: **Statistics** and **I/F Statistics**. Selecting the **Statistics** option will launch the highest level of statistics available for the selected interface: if the interface supports RMON, the RMON statistics window will display; if the interface does not support RMON, or if the RMON Default MIB component has been administratively disabled, the MIB-II I/F Statistics window will display. Selecting the **I/F Statistics** option will always display MIB-II interface statistics, regardless of the level of RMON support available or the current administrative status of the RMON Default MIB component.

Tthe MIB-II I/F Statistics window is also available for all port interfaces — regardless of their level of RMON support or the current administrative status of the RMON Default MIB component — via the I/F Summary window accessed from the Device menu, and via the I/F Statistics option on the bridge Port menu in the Bridge Status view. For more information about the I/F Summary window, see ***Chapter 3****; for more information about the Bridge Status view, see the* **Tools Guide**.

Accessing the Statistics Windows

1. Click on the desired **port index** in the Device Logical View window. The Port menu will appear.
2. **For RMON statistics** (where available), click to select **Statistics**. The RMON Statistics (Figure 3-1) or MIB-II I/F Statistics (Figure 3-3) window, as appropriate, will appear.

   or

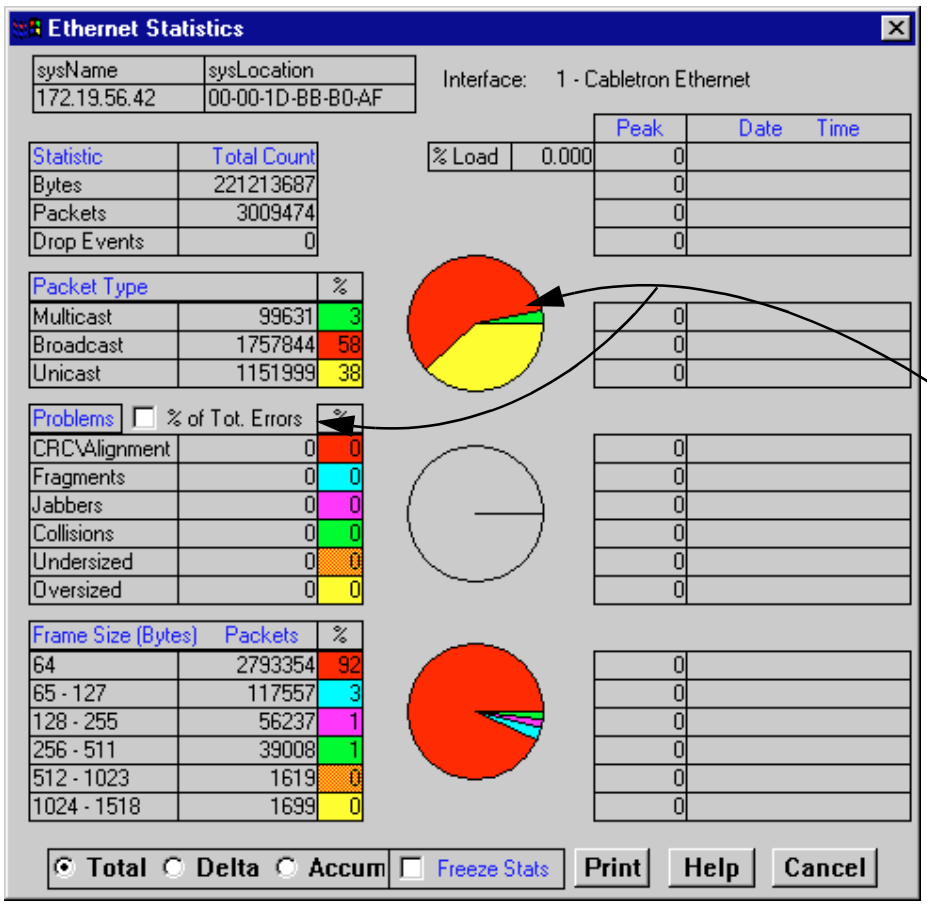
   For MIB-II interface statistics, click to select **I/F Statistics**. The MIB-II I/F Statistics window (Figure 3-3) will appear.

NOTE

If the selected interface displays MIB-II I/F Statistics and you were expecting to see RMON statistics, the RMON Default MIB component may be disabled; see the **RMON User's Guide** *for information on how to check (and if necessary, change) the admin status of the RMON Default MIB component.*

RMON Statistics

The RMON Ethernet Statistics window (Figure 3-1) provides a detailed statistical breakdown of traffic on the monitored Ethernet network. Statistics are provided in both numerical and graphic format, and include peak values and the date and time they occurred.



The Errors pie chart will only be display ed when the ***% of Tot. Errors*** *option is selected.*

Figure 3-1. The Ethernet Statistics Window

The selected interface number and its description are displayed at the top of the Statistics window. The column on the left side of the window displays each statistic's name, total count, and percentage; the column on the right displays the peak value for each statistic, and the date and time that peak occurred. Note that peak values are always Delta values; see **Viewing Total, Delta, and Accumulated Statistics**, on page 3-5, for more information.

The Ethernet statistics are as follows:

Bytes
Displays the total number of bytes contained in packets processed on the network segment. This number includes bytes contained in error packets.

Packets
Displays the total number of packets processed on the network segment. Again, this number includes error packets.

Drop Events
This field indicates the number of times packets were dropped because the device could not keep up with the flow of traffic on the network. Note that this value does not reflect the number of packets dropped, but only the number of times packets were dropped.

% Load
Displays the network segment load during the sample interval, in hundredths of a percent; this percentage reflects the network segment load compared to the theoretical maximum load (10/100 Mbps) of an Ethernet network.

Packet Type

Multicast	Indicates the number of good packets processed on the network segment that were destined for more than one address. Note that this total does not include broadcast packets.
Broadcast	Indicates the number of good packets processed on the network segment that had the broadcast (FF-FF-FF-FF-FF-FF) destination address.
Unicast	Indicates the number of good packets processed on the network segment that were destined for a single address.

The percentages displayed to the right of the numerical values for these fields indicate what percentage of good packets transmitted on the network segment were multicast, broadcast, and unicast; these percentages will add up to 100. The pie chart in the center of the window provides a graphical view of the percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.

Problems

CRC / Alignment	Indicates the number of packets processed by the network segment that had a non-integral number of bytes (alignment error) or a bad frame check sequence (Cyclic Redundancy Check, or CRC error).
Fragments	Indicates the number of packets processed by the network segment that were undersized (less than 64 bytes in length; a runt packet) ***and*** had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).
Jabbers	Indicates the number of packets processed by the network segment that were oversized (greater than 1518 bytes; a giant packet) ***and*** had either a non-integral number of bytes (alignment error) or a bad frame check sequence (CRC error).
Collisions	Indicates the total number of **receive** (those the device detects while receiving a transmission) and **transmit** (those the device detects while transmitting) collisions detected on the network segment.
Undersized	Indicates the number of packets processed by the network segment that contained fewer than 64 bytes (runt packets) but were otherwise well-formed.
Oversized	Indicates the number of packets processed by the network segment that contained more than 1518 bytes (giant packets) but were otherwise well-formed.

In their default state, the percentages displayed to the right of the numerical values for these fields indicate what percentage of **total packets** transmitted on the network segment were of the noted type. If you select the **% of Tot. Errors** option by clicking the mouse button in the check box, the percentages will indicate what percentage of **problem**, or **error**, **packets** transmitted on the network segment were of the noted type; these percentages will add up to 100. (The **% of Tot. Errors** option is active if there is an X in the check box.) The pie chart in the center of the window provides a graphical view of the selected percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.

Frame Size (Bytes) Packets

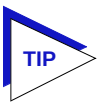
The Frame Size (Bytes) Packets fields indicate the number of packets (including error packets) processed by the network segment that were of the noted length, excluding framing bits but including frame check sequence bits. Packet sizes counted are:

- 64
- 65-127
- 128-255
- 256-511
- 512-1023
- 1024-1518

The percentages displayed to the right of the numerical values for these fields indicate what percentage of all packets transmitted on the network segment were of the noted size. Unless the network segment has experienced a significant number of runts and/or giants (which are not counted in this group), these percentages will add up to 100. The pie chart in the center of the window provides a graphical view of the percentage breakdown; colors in the pie chart correspond to colors in the percentage display boxes. Values listed to the right of the pie chart indicate peak delta values recorded since the statistics screen was launched, and the date and time they occurred.

Viewing Total, Delta, and Accumulated Statistics

By using the **Total**, **Delta**, and **Accum** option buttons located at the bottom of each Statistics window, you can choose whether to view the total statistics count (since the last time the device was initialized), the statistics count during the last polling interval, or a fresh accumulation of statistics begun when the **Accum** button was selected.



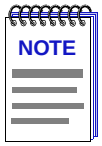
The statistics windows use the polling interval you have set for the monitored device via the Device Management page of the Options window. See the **User's Guide** *for more information on setting the Chassis Manager polling interval.*

To choose **Total**, **Delta**, or **Accum**:

1. Click on the **Total** option button; after the completion of the current polling cycle plus one complete polling cycle, the screen will display the total count of statistics processed since the entry was created or since the device was last initialized, whichever is most recent. These totals are updated after each polling cycle.
2. Click on the **Delta** option button; after the completion of the current polling cycle plus two more polling cycles, the screen will display the count of statistics processed during the last polling interval. These counts will be refreshed after each polling cycle.

3. Click on the **Accum** option button; after the completion of the current polling cycle plus two more polling cycles, the screen will display a fresh cumulative count of statistics. Note that making this selection does ***not*** clear device counters; you can still re-select **Total** for the total count since the device was last initialized.

Switching the statistics displays among **Total**, **Delta**, and **Accum** does not effect the displayed peak values, as peak values are always **Delta** values.



If you reset your device, you must first close, then re-open the Statistics window to refresh peak values.

To temporarily freeze the statistics display, select the **Freeze Stats** option; in this mode, statistics will continue to be collected, but the display will not update. To resume normal updates, click again to de-select the freeze option.

Printing Statistics

The **Print** button located at the bottom of the Statistics window allows you to print the current snapshot of statistical data. When you select **Print**, a standard Windows Print window like the sample shown in Figure 3-2 will appear.

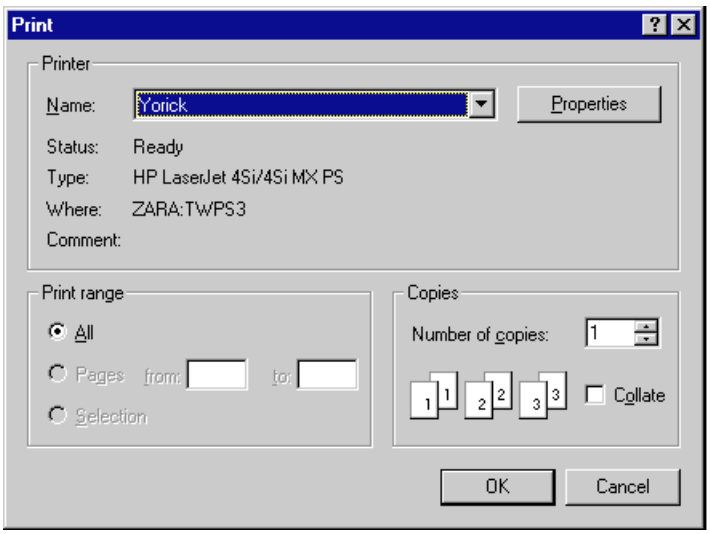


Figure 3-2. Standard Print Window

Adjust printer settings as required, then click **OK**.

Interface Statistics

The interface I/F Statistics window (Figure 3-3) provides MIB-II interface statistical information — including counts for both transmit and receive packets, and error and buffering information — for the front panel interfaces on the MultiSwitch 700 module. Color-coded pie charts in the middle of the window let you graphically view statistics for Unicast, Non-Unicast, Discarded and Error packets.

TIP

*This window can also be launched from the **I/F Statistics** option on the Device Logical View port menus; from the **Statistics** option if the selected interface does not support RMON or if the RMON Default MIB component has been administratively disabled. This window is also available for all port interfaces via the I/F Summary window (described in **Chapter 3**) or the Bridge Port menus in the Bridge Status view (see the* **Tools Guide**).

To access the interface's I/F Statistics window:

1. In the Device Logical View window, click on the appropriate port interface to display the Port menu.
2. Select **I/F Statistics**. The MIB-II I/F Statistics window will appear.

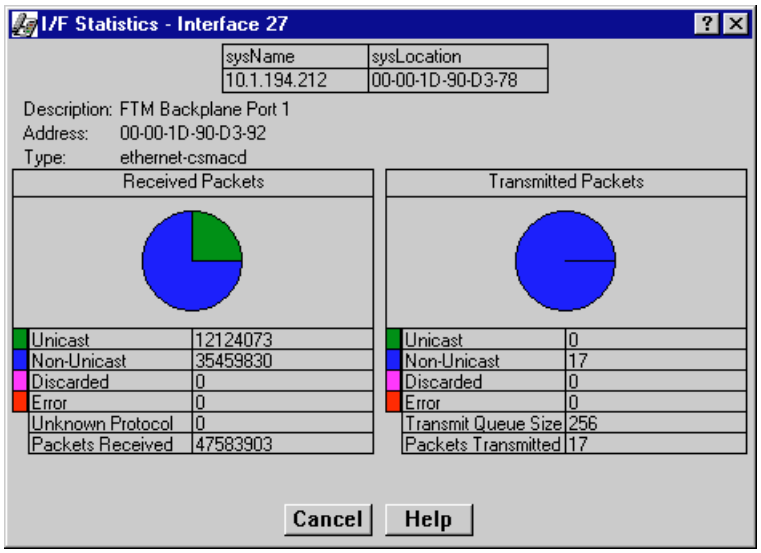


Figure 3-3. The Interface Statistics Window

Three informational fields appear in the upper portion of the window:

Description
Displays the interface description for the currently selected interface (e.g., Enet, Fast Enet, FDDI, ATM, or Backplane Port).

Address
Displays the MAC (physical) address of the selected interface.

Type
Displays the interface type of the selected port: e.g., ethernet-csmacd, fddi, or atm.

The lower portion of the window provides the following transmit and receive statistics; note that the first four statistics are also graphically displayed in the pie charts.

Unicast
Displays the number of packets transmitted to or received from this interface that had a single, unique destination address. These statistics are displayed in the pie chart, color-coded green.

Non-Unicast
Displays the number of packets transmitted to or received from this interface that had a destination address that is recognized by more than one device on the network segment. The multicast field includes a count of broadcast packets — those that are recognized by *all* devices on a segment. These statistics are displayed in the pie chart, color-coded dark blue.

Discarded
Displays the number of packets which were discarded even though they contained no errors that would prevent transmission. Good packets are typically discarded to free up buffer space when the network becomes very busy; if this is occurring routinely, it usually means that network traffic is overwhelming the device. To solve this problem, you may need to re-configure your bridging parameters, or perhaps re-configure your network to add additional bridges or switches.

These statistics are displayed in the pie chart, color-coded magenta.

Error
Displays the number of packets received or transmitted that contained errors. These statistics are displayed in the pie chart, color-coded red.

Unknown Protocol *(Received only)*
Displays the number of packets received which were discarded because they were created under an unknown or unsupported protocol.

Packets Received *(Received only)*
Displays the number of packets received by the selected interface.

Transmit Queue Size *(Transmit only)*
Displays the number of packets currently queued for transmission from this interface. The amount of device memory devoted to buffer space, and the traffic level on the target network, determine how large the output packet queue can grow before the MultiSwitch 700 module will begin to discard packets.

Packets Transmitted *(Transmit only)*
Displays the number of packets transmitted by this interface.

Making Sense of Interface Statistics

The statistics available in this window can give you an idea of how an interface is performing; by using the statistics in a few simple calculations, it's also possible to get a sense of an interface's activity level:

To calculate the percentage of input errors:

```
Received Errors /Packets Received
```

To calculate the percentage of output errors:

```
Transmitted Errors /Packets Transmitted
```

To calculate the total number of inbound and outbound discards:

```
Received Discards + Transmitted Discards
```

To calculate the percentage of inbound packets that were discarded:

```
Received Discards /Packets Received
```

To calculate the percentage of outbound packets that were discarded:

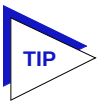
```
Transmit Discards /Packets Transmitted
```

Chapter 4

Alarm Configuration

Accessing the Basic and Advanced Alarms windows; creating a basic alarm; creating an advanced alarm; creating events; assigning actions to events; viewing the event log

Through the RMON Alarm and Event functionality supported by your MultiSwitch 700 module, you can configure alarms and events (and, where appropriate, actions) for each available interface.



The Alarm, Event, and Actions windows described in this chapter are identical to those provided via the RMON utility. For more information about other features of RMON, see the **RMON User's Guide**.

About RMON Alarms and Events

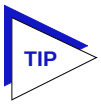
Although Alarms and Events are defined as separate RMON groups, neither one can function properly without the other: you can define an alarm threshold, but if it doesn't point to an event, there will be no indication that the threshold has been crossed; similarly, you can define an event, but unless it is attached to an alarm threshold, it won't be triggered. Each is an essential part of the same notification process: the alarm defines a set of conditions you want to know about, and the event determines the means of letting you know those conditions have occurred.

Events are also an integral part of the filter and packet capture functionality: you can start and stop packet capturing in response to events, or a successful packet capture can generate its own event.

NetSight Element Manager provides two means for configuring RMON alarms: using the Basic Alarms window, you can define both rising and falling alarm thresholds for up to three pre-selected MIB-II variables per interface; based on the options you select, the application automatically creates the necessary events (to log alarm occurrences, generate a trap, or both) and — for devices which support the Cabletron-proprietary Actions MIB — adds the requested actions to those events (to enable or disable bridging at the selected interface).

Using the Advanced Alarms feature, you can define custom alarms for almost any MIB-II or RMON object, as long as it is present in the device firmware and its value is defined as an integer (including counters, timeticks, and gauges). All aspects of these alarms are user-selectable: thresholds can be established on either the absolute or delta value for a variable; events can be configured to create a log, generate a trap, or both; and for devices that support the new Actions MIB, events can also be configured to perform any defined SNMP SET or series of SETs on device objects. The Advanced Alarms feature also allows you to configure any events you wish to use in conjunction with the Packet Capture functionality. (For more information on using the Packet Capture feature, see the ***RMON User's Guide***.)

The Basic Alarms feature allows you to assign alarms to any interface type; using the Advanced Alarms feature, you need only be sure to select variables appropriate to the interface — Ethernet for Ethernet, Token Ring for Token Ring, etc. — when defining your alarms.



As long as there is at least one Ethernet or Fast Ethernet module installed in your MultiSwitch 700 chassis, you can use the RMON Alarms feature to configure alarms for MIB objects on FDDI, ATM, and other interfaces that don't specifically support RMON: the Basic Alarms window provides MIB II objects as alarm variables; Advanced Alarm configuration allows you to select any object as an alarm variable, as long as its value is defined as an integer and you assign the correct instance value. See step 5 on page 4-18 and the Note which follows it for more information on assigning the correct instance value to an advanced alarm.

Basic Alarm Configuration

Using the Basic Alarm Configuration application, you can define both rising and falling alarm thresholds for three selected MIB-II objects: *ifInOctets*, *ifInNUcastPkts*, and *ifInErrors*. Because these pre-selected objects are not RMON-specific, you can configure alarms for all interfaces installed in your MultiSwitch 700 module — including those, like FDDI, for which no specific RMON statistics currently exist.

In addition to configuring separate rising and falling thresholds, you can also configure your device's *response* to an alarm condition. When a threshold is crossed, the RMON device can create a log of alarm events, send a trap notifying your management workstation that an alarm condition has occurred, or both. You can even configure an alarm to enable or disable bridging on the offending port in response to a rising or falling alarm condition.

The Basic Alarm Configuration window combines the three parts of creating a working alarm — configuring the alarm itself, configuring an event that will announce the occurrence of an alarm (including assigning any actions), and linking the two — into a single step, and handles the details transparently. For more information about the individual steps involved in creating an alarm, see ***Advanced Alarm Configuration****, on page 4-10.*

Accessing the Basic Alarm Configuration Window

To access the RMON Basic Alarm Configuration window:

1. From the Chassis Logical View, click on the appropriate **port index** to display the Port menu.
2. Select **Alarm Configuration**. The RMON Basic Alarm Configuration window, Figure 4-1 on the following page, will appear.

When the window is first launched, no interfaces will be selected, and the **Apply**, **Disable**, and **View Log** buttons will be grayed out. **Apply** and **Disable** will activate when an interface is selected; **View Log** will activate when an interface which has experienced an alarm event is selected. The presence of an event log is indicated by the double greater-than sign (>>) displayed to the left of the threshold value that was crossed.

Viewing Alarm Status

The Basic Alarm Configuration window contains all the fields you need to configure one or more of the three basic alarms available for each interface installed in your RMON device:

Kilobits — Total Errors — Broadcasts/Multicasts

Use these fields at the top of the window to change the alarm type displayed in the list box. For example, if the **Kilobits** option is selected, the information in the list box pertains to the status of the Kilobits alarm type for each installed interface. Before you configure an alarm or alarms, be sure the appropriate option is selected here.

The available alarm variables are:

- **Kilobits** *(ifInOctets)* — tracks the number of octets of data received by the selected interface. Note that this value has been converted for you from octets (or bytes) to kilobits (or units of 125 bytes); be sure to enter your thresholds accordingly. For example, to set a rising threshold of 1250 octets, enter a threshold value of 10; to set a falling threshold of 625 octets, enter a threshold value of 5.

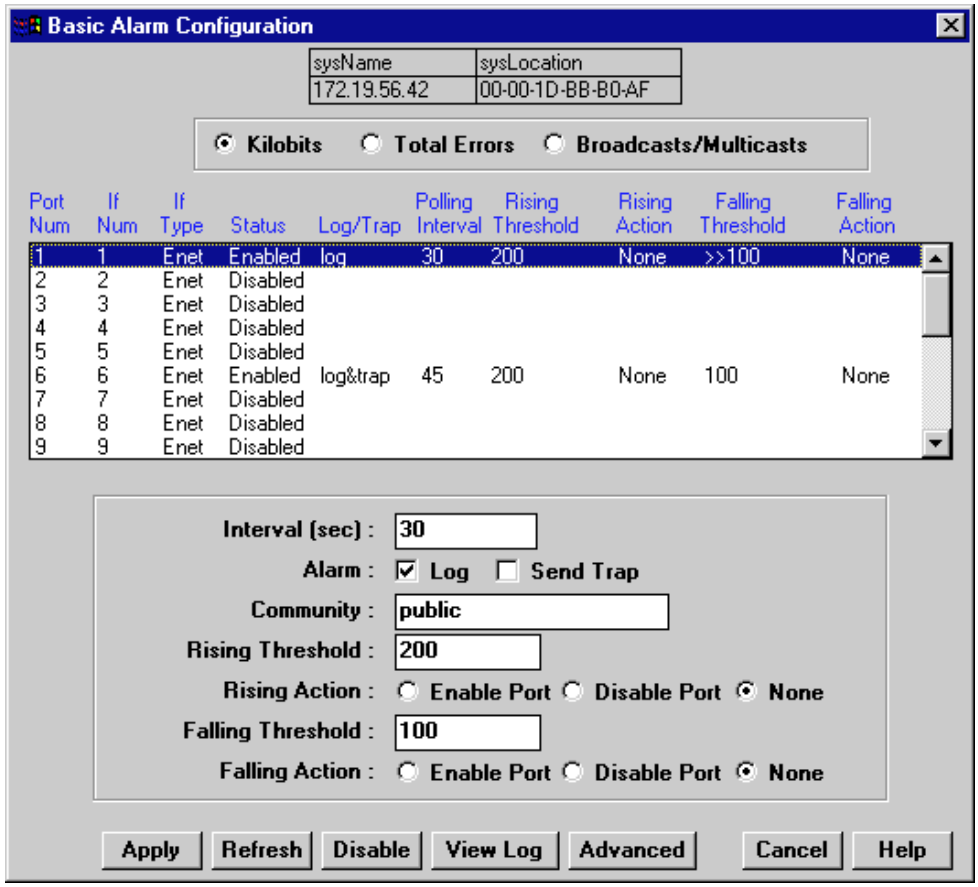


Figure 4-1. RMON Basic Alarm Configuration Window

- **Total Errors** *(ifInErrors)* — tracks the number of error packets received by the selected interface.
- **Broadcast/Multicast** *(ifInNUcastPkts)* — tracks the number of non-unicast — that is, broadcast or multicast — packets received by the selected interface.

TIP

The three pre-selected alarm variables are all MIB II variables; this allows you to configure alarms for any installed interface — even those for which no specific RMON statistics exist.

Port Number

Provides a sequential indexing of the interfaces installed in your RMON device.

IF Number

Displays the interface number assigned to each available interface.

IF Type
Displays each interface's type: FDDI, Ethernet, Token Ring, or ATM. Note that there is no type distinction between standard Ethernet and Fast Ethernet.

Status
Displays the current status of the selected alarm type for each interface: Enabled or Disabled. Remember, this status refers only to the alarm type which is selected at the top of the window; each of the other two alarm types can have different states.

Log/Trap
Indicates whether or not each alarm has been configured to create a silent log of event occurrences and the alarms that triggered them, and whether or not each alarm has been configured to issue a trap in response to a rising or falling alarm condition. Possible values are **log**, **trap**, **log&trap**, or **none**.

Polling Interval
Displays the amount of time, in seconds, over which the selected alarm variable will be sampled. At the end of the interval, the sample value will be compared to both the **Rising Threshold** and **Falling Threshold** (described below). You can set any interval from 1 to 65,535 seconds.

Rising Threshold
Displays the high threshold value set for the selected alarm variable. Values used to compare to the thresholds are relative, or **delta** values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Rising Action
These option buttons indicate whether or not a rising alarm occurrence will initiate any actions in response to the alarm condition: **Enable Port** if bridging will be enabled at the selected interface in response to a rising alarm, **Disable Port** if bridging will be disabled at the selected interface in response to a rising alarm, or **None** if no actions have been configured for the selected alarm. The Action fields will be unavailable for devices that do not support the new Actions MIB.

Falling Threshold
Displays the low threshold value set for the selected alarm variable. Values used to compare to the thresholds are relative, or **delta** values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

Falling Action

These option buttons indicate whether or not a falling alarm occurrence will initiate any actions in response to the alarm condition: **Enable Port** if bridging will be enabled at the selected interface in response to a falling alarm, **Disable Port** if bridging will be disabled in response to a falling alarm, or **None** if no actions have been configured for the selected alarm. The Action fields will be unavailable for devices that do not support the new Actions MIB.

Before you decide whether or not to assign an action to a rising or falling alarm, it is important to understand something about the hysteresis function built in to the RMON alarm functionality. See ***How Rising and Falling Thresholds Work****, on page 4-27, for more information.*

The remainder of the window fields provide the means for configuring alarms for each available interface. The information provided in this screen is static once it is displayed; for updated information, click on the **Refresh** button. Adding or modifying an alarm automatically updates the list.

Creating and Editing a Basic Alarm

The editable fields at the bottom of the Basic Alarm Configuration window allow you to configure alarm parameters for each available interface. These fields will display the parameters used for the most recently configured alarm (no matter which interfaces are selected in the list box); this allows you to set the same parameters on multiple interfaces with a single set. Hold down the **Shift** key while clicking to select a contiguous group of interfaces; use the **Ctrl** key to select any interfaces. To display the alarm parameters for a specific interface, double-click on that interface.

There is no specific "Enable" function; simply configuring thresholds and/or actions for an alarm and applying those changes enables the alarm. For more information on disabling an alarm, see **Disabling a Basic Alarm**, page 4-9.

To configure an alarm:

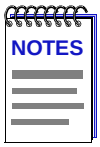
1. At the top of the window, click to select the variable to be used for your alarm: **Kilobits**, **Total Errors**, or **Broadcast/Multicast**. The display in the list box will reflect the current status at each interface of the alarm type you have selected.
2. In the list box, click to highlight the interface (or use **shift-click** or **ctrl-click** to select multiple interfaces) for which you would like to configure an alarm for the selected variable. Note that the editable fields will display the parameters assigned to the most recently set alarm; however, any changes you make in these fields will be set to *all* selected interfaces.

3. In the **Interval** field, enter the amount of time, in seconds, over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. You can assign any interval from 1 to 65,535.

4. In the **Alarm** field, click to select one or both of the following options:

   a. Select **Log** if you wish to create a silent log of alarm occurrences.

   b. Select **Send Trap** if you want your device to issue a trap in response to each alarm occurrence.



In order for the trap selection to work properly, your MultiSwitch 700 module must be configured to send traps to your network management station. This is accomplished via Local Management or the Remote Administration Tools application. Consult your device hardware manual or the **Remote Administration Tools User's Guide** *for details.*

If you are monitoring a variable you consider to be critical, we do not recommend that you select ***Trap*** *as the only event response; if a trap is lost due to a collision or other transmission problem, it will not be re-sent.*

5. Any value you enter in the **Community** field will be included in any trap messages issued by your MultiSwitch 700 module in response to the alarm(s) you are configuring. This value is also used to direct traps related to this alarm to the appropriate management workstation(s):

   a. **If you enter a value in this field**, traps related to the associated alarms will only be sent to the network management stations in the device's trap table *which have been assigned the same community name* (and for which traps have been enabled). Any IP addresses in the device's trap table which have *not* been assigned the same community string, or which have been assigned no community string, will not receive traps related to the alarm(s) you are configuring.

   b. **If you leave this field blank**, traps related to the associated alarms will be sent to any network management stations which have been added to the device's trap table, and for which traps have been enabled — regardless of whether or not those IP addresses have been assigned a community name in the trap table.

6. Click in the **Rising Threshold** field, and enter the high threshold value for this alarm. Remember, compared values are always relative, or delta values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

   When configuring a **Kilobits** alarm, NetSight Element Manager converts octets into kilobits (units of 125 bytes, or octets) for you;
   for example, to set a rising threshold of 1250 octets, enter a threshold value of 10.

7. In the **Rising Action** field, click to select the action you want your device to take in response to a rising alarm: Enable Port, Disable Port, or None. Note that this action enables or disables only *bridging* at the specified port, and not the interface itself.

   For more information on how actions are triggered, see **How Rising and Falling Thresholds Work**, on page 4-27.

8. Click in the **Falling Threshold** field, and enter the low threshold value for this alarm. Remember, compared values are always relative, or delta values (the difference between the value counted at the end of the current interval and the value counted at the end of the previous interval); be sure to set your thresholds accordingly.

   When configuring a **Kilobits** alarm, NetSight Element Manager converts octets into kilobits (units of 125 bytes, or octets) for you; for example, to set a falling threshold of 625 octets, enter a threshold value of 5.

9. In the **Falling Action** field, click to select the action you want your device to take in response to a falling alarm: Enable Port, Disable Port, or None. Note that this action enables and disables only *bridging* at the specified port, and not the interface itself.

   For more information on how actions are triggered, see **How Rising and Falling Thresholds Work**, page 4-27.

The Actions fields will be grayed out for devices that do not support the proprietary Actions MIB.

10. Click the **Apply** button to set your changes. If you have made any errors in configuring alarm parameters (using an invalid rising or falling threshold, for example, or neglecting to supply a polling interval), either an error window with the appropriate message will appear, or a beep will sound and the cursor will blink in the field which contains the error. Correct the noted problem(s), and click **Apply** again.

Once you click the **Apply** button, the configured alarm parameters will be set for every selected interface, and the alarms will automatically be enabled; the list box display will also refresh to reflect these changes.

To configure additional alarms, or alarms of a different type, select the appropriate alarm variable at the top of the window, highlight the appropriate interface(s), and repeat the procedures outlined above.

Disabling a Basic Alarm

Using the **Disable** button at the bottom of the window actually performs two functions: it both disables the alarm and deletes the alarm entry (and its associated event and action entries) from device memory to help conserve device resources. In the list box display, the parameters for any "disabled" alarm are automatically reset to their default values.

1. In the top of the window, click to select the variable for which you wish to disable an alarm: **Kilobits**, **Total Errors**, or **Broadcast/Multicast**.
2. In the list box display, click to highlight the interface(s) for which you wish to disable the selected alarm type. (Remember, you can use **shift-click** to select a sequential group of interfaces, or **ctrl-click** to select any group of interfaces.)
3. Click on the **Disable** button. The selected alarm type on the selected interface(s) will be disabled, and the list box display will refresh to reflect those changes.

Viewing the Basic Alarm Log

If you have selected the "log" response for an alarm, and that alarm's rising and/or falling threshold has been crossed, the Basic Alarms application will create a log of alarm occurrences. If a threshold has been crossed, it will be preceded in the interface list box display by a double greater-than sign (>>). Clicking to select an interface which is so marked will activate the **View Log** button; selecting the **View Log** button will launch the appropriate Basic Alarm Log, Figure 4-2. (Selecting more than one interface — even if all selected interfaces have experienced alarm conditions — will inactivate the **View Log** button; you can only view a single alarm log at a time.)

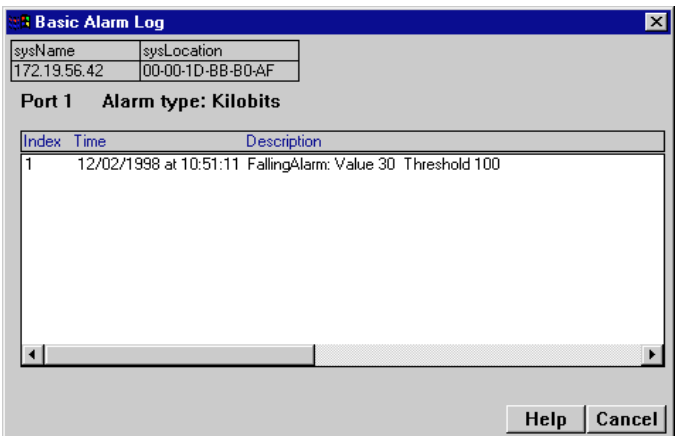
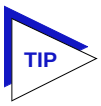


Figure 4-2. Basic Alarm Log

The top portion of the Basic Alarm Log window contains the device information boxes, as well as the Port Number assigned to the interface that experienced the alarm condition and the type of alarm that was triggered; the remainder of the window contains the following information about each alarm occurrence:

Index	This index number uniquely identifies each *occurrence* of a rising or falling event. Note that, since the alarm whose log is displayed in Figure 4-2 experienced both rising and falling alarms, there are two sets of event indices: one which identifies each instance of the rising alarm, and one which identifies each instance of the falling alarm.



For more information about the relationship between rising and falling alarms and the hysteresis function that controls the generation of alarm events, see ***How Rising and Falling Thresholds Work****, on page 4-27.*

Time	Indicates the date and time of each event occurrence.
Description	Provides a detailed description of the condition which triggered the alarm, including whether it was a Rising or Falling alarm, the Value which triggered the alarm, and the configured Threshold that was crossed.

Each log will hold only a finite number of entries, which is determined by the resources available on the device; when the log is full, the oldest entries will be replaced by new ones.

Advanced Alarm Configuration

The Basic Alarm Configuration window provides a quick and easy way to set up some basic alarms for all of the interfaces on your MultiSwitch 700 module. However, if you prefer more control over the parameters of the alarms you set (as well as their associated events and actions) and/or a wider array of choices for each variable, the Advanced Alarm feature provides a powerful and flexible means for configuring alarms, events, and actions to suit your particular networking needs.

Accessing the RMON Advanced Alarm/Event List

To access the RMON Advanced Alarm/Event List window:

1. From the Device View, click on the appropriate port interface to display the Port menu; select **Alarm Configuration**.
2. In the Basic Alarm Configuration window, click on the **Advanced** button; the RMON Advanced Alarm/Event List window, Figure 4-3, will appear.

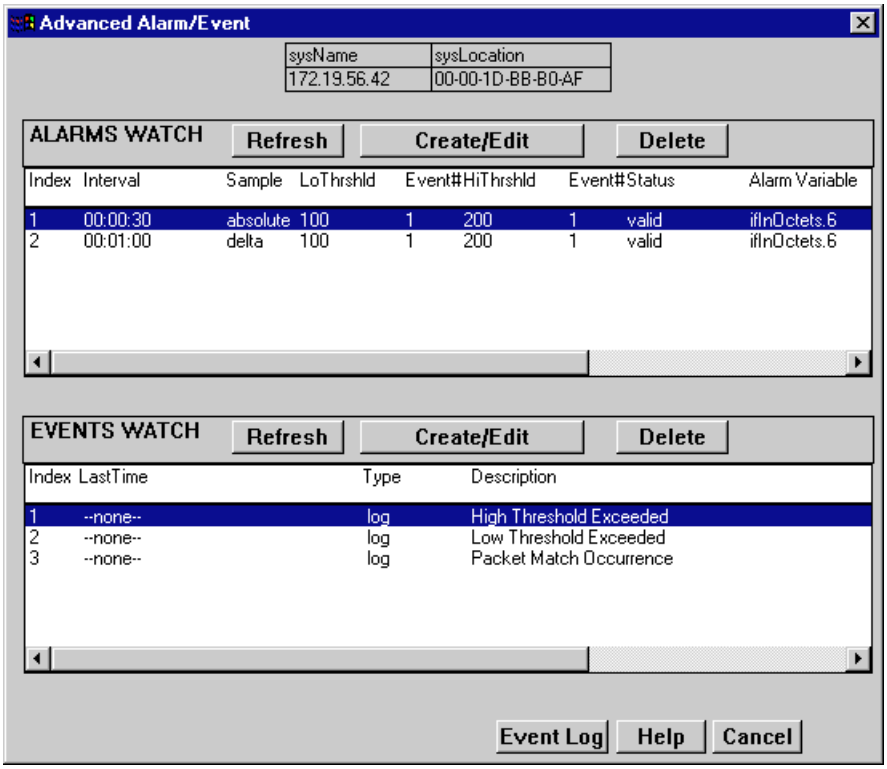


Figure 4-3. The RMON Advanced Alarm / Event List Window

NOTES

Neither the Alarms or Events list is interface-specific; both will be displayed the same for every interface.

Alarms and events which have been configured via the Basic Alarms window are not displayed in and cannot be accessed or edited from the Advanced Alarm/Event List window.

The top portion of the window displays the usual device information boxes; the remainder of the window contains the Alarms Watch and Events Watch lists, and the command buttons that allow you to create, edit, and delete entries in those lists, or refresh the display.

The fields in the Alarms Watch display include:

Index	The index is a number that uniquely identifies each alarm. Index numbers are user-defined; you can use any indexing scheme that works for you. These numbers are permanently assigned to their associated alarms; however, index numbers made available by the deletion of existing alarms can be assigned to new alarms, as needed. Indices 2000 to 3999 are reserved and unavailable.
Interval	Indicates the amount of time, in seconds, over which the selected variable will be sampled. At the end of the interval, the sample value is compared to both the rising and falling thresholds configured for the alarm.
Sample	Indicates whether the sample value to be compared to the thresholds is an **absolute**, or total value — that is, the total value counted for the selected variable during the interval — or a relative, or **delta** value — the difference between the value counted during the current interval and the value counted during the previous interval.
LoThrshld	Indicates the set value for the low, or falling threshold.
Event #	Indicates the event index number that the falling threshold points to: this is the event that will be triggered if the falling threshold is met or crossed. If the value for this field is zero, no event will be triggered.
HiThrshld	Indicates the set value for the high, or rising threshold.
Event #	Indicates the event index number that the rising threshold points to: the event that will be triggered if the rising threshold is met or crossed. If the value for this field is zero, no event will be triggered.
Status	Indicates the status of the alarm: valid, invalid, or underCreation. An alarm that is invalid is not functional; it may be referring to a MIB component that is inactive (such as the Hosts component), not present, or unreachable, or it may have been deleted by software but not yet removed from memory at the device. An alarm that is underCreation is in the process of being configured (possibly by another management station), and should not be modified until its status is valid; if it never reaches valid status, it will eventually be removed.
Alarm Variable	Indicates the variable that is being watched. You can use the scroll bar, if necessary, to view the complete name.

The information provided in this screen is static once it is displayed; for updated information, click on the **Refresh** button. Adding or modifying an alarm automatically updates the list.

The fields in the Events Watch display include:

Index	This is a number that uniquely identifies an entry in the event table; an index number is assigned when an event is created. These numbers are extremely important, as they are the means by which an event is associated with an alarm or a packet capture filter. As with alarms, these index numbers are user-defined and can be assigned according to any indexing scheme that works for you. Index numbers are permanently assigned to their associated events; however, numbers made available by the deletion of existing events can be assigned to new events, as needed. Note that indices 2000 to 4999 are reserved and unavailable.
LastTime	Indicates the last time this event was triggered. Note that this information is static once it is displayed, and the LastTime field will not be updated unless you close, then open, the Advanced Alarms/Events window, or click on the **Refresh** button.
Type	Indicates the type of response that will be generated if the event is triggered: log, trap, or log & trap. A type of "none" indicates that occurrences of the event will not be logged and no trap will be sent; however, note that this field does not indicate whether or not there are any actions associated with the selected event.
Description	This is a user-defined text description used to identify the event and/or the alarm or packet capture that triggers it.

The **Event Log** button at the bottom of the screen provides access to the log which lists the occurrences of an event.

The information provided in this screen is static. For updated information, click the **Refresh** button. Adding or modifying an event automatically updates the list.

Creating and Editing an Advanced Alarm

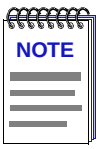
The Create / Edit Alarms window (Figure 4-4, page 4-15) allows you to both create new alarms and edit existing ones. When you click on the **Create/Edit** button in the Alarms Watch list, the Create / Edit Alarms window will display the parameters of the alarm which is currently highlighted in the list. (If no alarms have yet been configured, a set of default parameters will be displayed.) All of these parameters are editable: to change an existing alarm, edit any parameter *except* the Index value; to create an entirely new alarm, simply assign a new Index number. The ability to assign index numbers allows you to quickly and easily create a number of similar alarms without having to close, then re-open the window or re-assign every parameter.

The main Alarm / Event window remains active while the Create / Edit Alarms window is open; to edit a different alarm (or use its settings as the basis of a new alarm), simply double-click on the alarm you want to use in the main Alarms Watch list, and the Create / Edit Alarms window will update accordingly.

To configure an alarm:

1. **If you wish to modify an existing alarm** or create a new alarm based on the parameters of an existing one, be sure the alarm of interest is highlighted in the Alarms Watch list, then click on the **Create/Edit** button at the top of the Alarms Watch portion of the RMON Advanced Alarm/Event window. The Create/Edit Alarms window, Figure 4-4, will appear.

   If you wish to create an entirely new alarm, it doesn't matter which existing alarm (if any) is highlighted when you open the Create/Edit Alarms window; although the window will, by default, display the parameters of whichever alarm is currently selected, all parameters are editable and can be configured as desired.



Whether you are modifying an existing alarm or creating a new one is determined solely by the assignment of the Index number: if you assign a previously unused index number, a new alarm instance will be created; if you use an existing index number, its associated alarm will be modified.

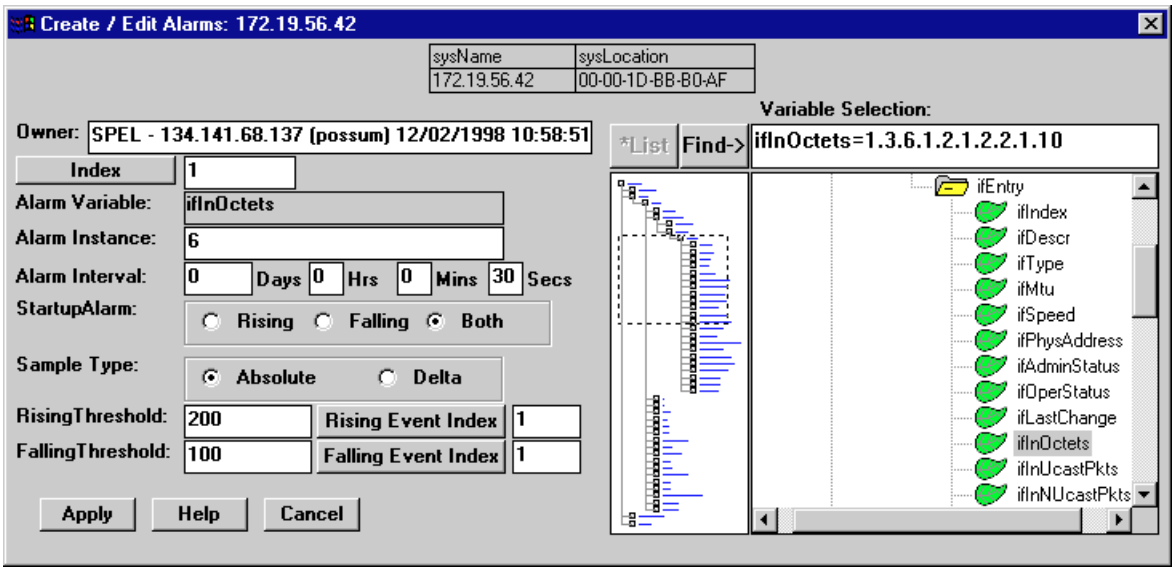


Figure 4-4. The RMON Create/Edit Alarms Window

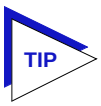
2. In the **Owner** text box, enter some appropriate text designation for this alarm, if desired; you may want to use the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the creator of the alarm. Since any workstation can access and change the alarms you are setting in your MultiSwitch 700 module, some owner identification can prevent alarms from being altered or deleted accidentally. The default value provided is — <IP address> <(hostname)> <date> <time>, where <IP address> and <(hostname)> refer to the workstation that created the alarm and <date> and <time> reflect the date and time of the alarm's creation.

3. **If you are creating a new alarm**, use the **Index** field to assign a unique, currently unused index number to identify the alarm. Clicking on the **Index** button will automatically assign the lowest available number; you can also click directly in the text box and assign any value you want between 1 and 1,999 and 4,000 and 6,5535 (indices 2000 to 3999 are reserved and unavailable).

NOTE

*Clicking on the **Index** button to select the next available index number will replace the current Owner string with the default value described above; if the default value is already in place, the date and time will be updated.*

If you wish to modify an existing alarm, enter the appropriate index value, or double-click on the alarm of interest in the Alarms Watch list (in the main Alarm/Event window).



The only thing that determines whether you are modifying an existing alarm or creating a new one is the assignment of the index number; be sure to assign this value appropriately.

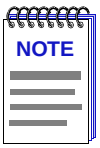
4. To select the **Variable** to be used for your alarm, use the MIB Tree display provided on the right side of the window. (For more information about how to use the MIB Tools utility, see the ***Tools Guide***.) The display will default to the top of the tree (labeled Internet); there are two ways to locate and/or assign the correct variable:

   a. If you know the exact name of the OID value you wish to track (including its capitalization), enter the name in the **Alarm Variable** field; to verify that you have entered the name correctly, click on the **Find->** button to move the MIB Tree display to that OID. (If the MIB Tree display does not adjust to show the OID you have entered, then you entered the name incorrectly; remember, the case must match exactly).

   b. Use the scroll bars and click to open the appropriate folders in the MIB Tree display to locate the object you wish you use; click to select it in the panel, and its name will automatically be entered in the **Alarm Variable** field.

If you don't know the exact spelling of the OID you wish to use for your alarm variable, and you can't find it by searching through the tree, use the MIB Tools utility's Find feature to locate the OID and determine its exact spelling (and tree location). For more information on the MIB Tools utility and its Find capabilities, see the **Tools Guide**.

Almost any RMON or MIB-II object can be used as an alarm variable as long as it is resident in the device firmware and its value is defined as an integer (including counters, timeticks, and gauges). If you select an invalid object (i.e., one whose value is not an integer), the message "!!Can't set alarm on this type!!" will display in the Alarm Variable field.



If you select an object which is not resident in the device firmware, you will receive a "Set Failed; ensure variable is readable" message when you try to set your alarm by clicking on the ***Apply*** *button. If you are unsure just which objects are resident on your device, and you find yourself receiving a lot of "Set Failed" messages, you can use the MIB Tools utility (accessed from the main console window menu bar or from a Device View) to determine which objects are and are not part of your device's firmware — simply query the object you are interested in; if the query response comes back empty, the object is not present (make sure you are using the appropriate community name when making a query, or you will get no response).*

5. Once you have selected the object you wish to use for your alarm variable, you must assign the appropriate instance value in the **Alarm Instance** field. Most RMON objects are instanced by the index number assigned to the table

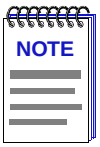
in which they reside; for example, if you wish to set an alarm on an object located in an RMON Statistics table, you can determine the appropriate instance by noting the index number assigned to the table that is collecting data on the interface you're interested in. In the case of the default tables, *index* numbers often mirror *interface* numbers; however, if there are multiple default tables per interface, or if additional tables have been created, this may not be true. (Table index numbers are assigned automatically as table entries are created; no two tables — even those on different interfaces — will share the same table index number.)

If you have selected an object from a table which is indexed by some other means — for example, by ring number — you must be sure to assign the instance accordingly. If you're not sure how a tabular object is instanced, you can use the MIB Tools utility (described in the ***Tools Guide***) to query the object; all available instances for the object will be displayed. (Host and matrix table objects — which are indexed by MAC address — require special handling; see the Note which follows this step, page 4-18.)

If you have selected an object which is *not* part of a table, you must assign an instance value of 0.

You can use the MIB Tree display to determine which objects are tabular and which are not: objects which are part of a table will descend from a ***blue*** *folder (which will have a "T" on it, and a name which will almost always include the word "table"); objects which are not will descend directly from a* ***yellow*** *folder. (There may be one or more yellow folders in between the blue folder which contains the table and the leaf object you wish to use; however, those objects are still part of the table.)*

Be sure you define your instance values carefully; if you neglect to set the instance correctly, you will receive the "Set failed; ensure variable is readable" error message when you click the **Apply** button to set your alarm.



If you wish to set an alarm on an object whose instance is non-integral — for example, a Host Table object indexed by MAC address — or on an object with multiple indices, like a Matrix Table entry (which is indexed by a pair of MAC addresses), you must follow certain special procedures for defining the instance. For these OIDs, the instance definition must take the following format:

table index.length(in bytes).instance(in decimal format)

For the first byte of the instance, you must use the index number of the ***table*** *which contains the OID you want to track. For example, to set an alarm on an object in the Host Table, define the first byte of the instance as the index number assigned to the specific Host Table you want to check. These index numbers are assigned automatically as the table entries are created; no two tables — even if they are on different interfaces — will share the same table index number.*

Second, you must specify the length, in bytes, of the index you will be using. Again, in the case of an object in the Host Table, that value would be 6, since Host Table entries are indexed by MAC address — a six-byte value.

Finally, you must specify the index itself, in ***decimal*** *format. In the case of a MAC address, that means you must convert the standard hexadecimal format to decimal format. To do this, simply multiply the first digit of the two-digit hex number by 16, then add the value of the second digit. (For hex values represented by alphabetical characters, remember that a=10, b=11, c=12, d=13, e=14, and f=15.) A hex value of b7, for instance, is represented in decimal format as 16 x 11 + 7, or 183.*

So, for example, the instance for an object in the Hosts group might read as follows:

2.6.0.0.29.170.35.201

where 2=the host table index; 6=the length in bytes of the index to follow; and 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9.

For objects with multiple indices — such as objects in a matrix table — you must add additional length and index information to the instance definition, as illustrated below:

3.6.0.0.29.170.35.201.6.0.0.29.10.20.183

where 3=the matrix table index; 6=the length in bytes of the index to follow; 0.0.29.170.35.201=the decimal format for MAC address 00-00-1d-aa-23-c9; 6=the length in bytes of the next index; and 0.0.29.10.20.183=the decimal format for MAC address 00-00-1d-0a-14-b7.

Additional instance issues may exist for FDDI objects; if you're unsure how to assign an instance, use the MIB Tools utility to query the object of interest, and note the appropriate instancing on the returned values.

6. In the **Alarm Interval** field, enter the amount of time over which the selected variable will be sampled. At the end of the interval, the sample value will be compared to both the rising and falling thresholds. There is no practical limit to the size of the interval (as the maximum value is 24,855 days 3 hours 14 minutes and 7 seconds — over 68 years!); the default value is 1 minute.

7. Since the first sample taken can be misleading, you can use the selections in the **Startup Alarm** box to disable either the rising or the falling threshold for that sample only. If you would like to exclude the falling alarm, select the **Rising** option; the first sample taken will only generate a rising alarm, even if the sample value is at or below the falling threshold. To exclude the rising alarm, select the **Falling** option; the first sample will then only generate a falling alarm, even if the sample value is at or above the rising threshold. If you wish to receive both alarms as appropriate, select the **Both** option.

8. Use the selections in the **Sample Type** box to indicate whether you want your threshold values compared to the total count for the variable during the interval (**Absolute**), or to the difference between the count for the current interval and the count for the previous interval (**Delta**). Make sure you have set your thresholds accordingly.

9. Click in the **RisingThreshold** field; enter the high threshold value for this alarm.

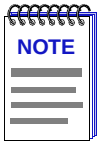
10. There are two ways to assign an event to your rising threshold: click in the **RisingEventIndex** text box and enter the number of the event you would like to see triggered if the rising threshold is crossed; or use the Events Watch list in the main Alarm/Event window to highlight the desired event, then click on the **Rising Event Index** button. Be sure you assign the number of a valid event or there will be no response if the selected variable meets or crosses this threshold; assigning an index of zero effectively disables the threshold, as there will be no indication that it has been crossed.

    For more information on how events are triggered, see **How Rising and Falling Thresholds Work**, on page 4-27.

11. Click in the **FallingThreshold** field; enter the low threshold value for this alarm.

12. There are two ways to assign an event to your falling threshold: click in the **FallingEventIndex** text box and enter the number of the event you would like to see triggered if the falling threshold is crossed; or use the Events Watch list in the main Alarm/Event window to highlight the desired event, then click on the **Falling Event Index** button. Again, be sure you assign the number of a valid event or there will be no response if the selected variable meets or crosses this threshold; assigning an index of zero effectively disables the threshold, as there will be no indication that it has been crossed.

    For more information on how events are triggered, see **How Rising and Falling Thresholds Work**, on page 4-27.



There is no limit to the number of alarms that may be assigned to the same event.

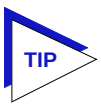
13. Click the **Apply** button to set your changes. If you have made any errors in configuring alarm parameters (using an invalid value in any field, leaving a field blank, or selecting an alarm variable which is not resident on the device), an error window with the appropriate message will appear. Correct the noted problem(s), and click the **Apply** button again.

The window remains open so that you may configure additional new alarms or modify existing ones; remember, you can double-click on any alarm in the Alarms Watch list in the main Alarm / Event window to display its parameters in the Create / Edit Alarms window. When you have finished configuring your alarms, click on the **Cancel** button to close the window.

Creating and Editing an Event

The Create / Edit Events window (Figure 4-5, on page 4-21) — like the Create / Edit Alarms window — allows you to both create new events and edit existing ones. When you click on the **Create/Edit** button in the Events Watch list, the Create / Edit Events window will display the parameters of the event which is currently highlighted in the list. (If no events have yet been configured, a set of default parameters will be displayed.) All of these parameters are editable: to change an existing event, edit any parameter *except* the Index value; to create an entirely new event, simply assign a new Index number. The ability to assign index numbers allows you to quickly and easily create a number of similar events without having to close, then re-open the window or re-assign every parameter.

The main Alarm / Event window remains active while the Create / Edit Events window is open; to edit a different event (or use its settings as the basis of a new event), simply double-click on the event you want to use in the main Events Watch list, and the Create / Edit Events window will update accordingly.



If the Create/Edit Actions window is also open, it too will update to display the actions associated with the event currently selected in the main Alarm/Event window. See ***Adding Actions to an Event****, on page 4-23, for more information on the actions feature.*

To configure an event:

1. **If you wish to modify an existing event** or create a new event based on the parameters of an existing one, be sure the event of interest is highlighted in the Events Watch list, then click on the **Create/Edit** button at the top of the Events Watch portion of the RMON Advanced Alarm/Event window. The Create/Edit Events window, Figure 4-5, will appear.

   If you wish to create an entirely new event, it doesn't matter which existing event (if any) is highlighted when you open the Create/Edit Events window; although the window will, by default, display the parameters of whichever event is currently selected, all parameters are editable and can be configured as desired.

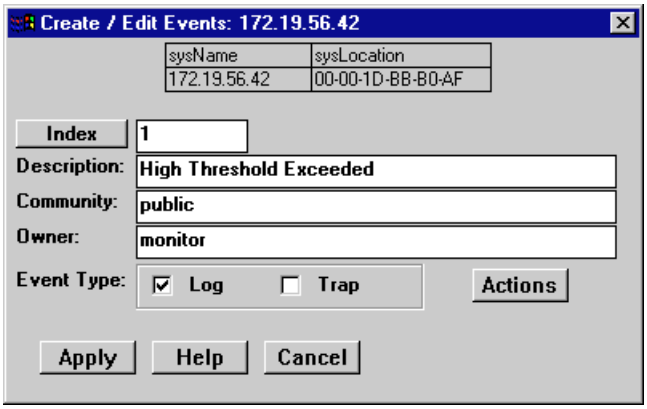


Figure 4-5. The RMON Create / Edit Events Window

TIP

Whether you are modifying an existing event or creating a new one is determined solely by the assignment of the Index number: if you assign a previously unused index number, a new event instance will be created; if you use an existing index number, its associated event will be modified.

2. **If you are creating a new event**, use the **Index** field to assign a unique, currently unused index number to identify the event. Clicking on the **Index** button will automatically assign the lowest available number; you can also click directly in the text box and assign any value you want between 1 and 1,999 and 5,000 and 65,534 (indices 2000 to 4999 are reserved and unavailable).

NOTE

*Clicking on the **Index** button to select the next available index number will replace the current Owner string with the default value; if the default value is in already in place, the date and time will be updated.*

If you wish to modify an existing event, enter the appropriate index value, or double-click on the event of interest in the Events Watch list (in the main Alarm/Event window).

TIP

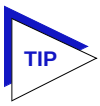
The only thing that determines whether you are modifying an existing event or creating a new one is the assignment of the index number; be sure to assign this value appropriately.

3. Click in the **Description** text box to enter any text description you want to identify the event. This description will appear in the Events Watch portion of the main Advanced Alarm/Event window, and help you distinguish among the events you have configured.

4. Any value you enter in the **Community** field will be included in any trap messages issued by your MultiSwitch 700 module when this event is triggered; this value is also used to direct traps related to this event to the appropriate management workstation(s):

   a. **If you enter a value in this field**, traps related to this event will only be sent to the network management stations in the device's trap table *which have been assigned the same community name* (and for which traps have been enabled). Any IP addresses in the device's trap table which have *not* been assigned the same community string, or which have been assigned no community string, will not receive traps related to the alarm(s) you are configuring.

   b. **If you leave this field blank**, traps related to this event will be sent to any network management stations which have been added to the device's trap table, and for which traps have been enabled — regardless of whether or not those IP addresses have been assigned a community name in the trap table.



For more information about configuring your MultiSwitch 700 module's trap table, consult your Local Management documentation or the **Remote Administration Tools User's Guide**. *(No traps will be sent by your MultiSwitch 700 module unless its trap table has been properly configured!)*

5. You can use the **Owner** text box for administrative or informational purposes; although the text entered here will not appear on any other windows, you may want to use the network manager's name or phone number, or the IP or MAC address of the management workstation, to identify the owner of the event. Since any workstation can access and change the events you are setting in your RMON device, some owner identification can prevent events from being altered or deleted accidentally. The default value provided is **monitor**.

6. Use the options in the **Event Type** field to define how this event will respond when an associated threshold is crossed:

   a. Select the **Log** option to create a silent log of event occurrences and the alarms that triggered them. Each event's log can be viewed by clicking on the **Event Log** button at the bottom of the Alarm/Event window. (See **Viewing an Advanced Alarm Event Log**, on page 4-26, for more information.)

   b. Select **Trap** to instruct the device to send a pair of SNMP traps (one WARNING, one NORMAL) to the management station each time the event is triggered.

NOTES

In order for the trap selection to work properly, your MultiSwitch 700 module must be configured to send traps to the management station. This is accomplished via local management or the Remote Administration Tools application; consult your device hardware manual or the **Remote Administration Tools User's Guide** *for details.*

If you are monitoring a variable you consider to be critical, we do not recommend that you select ***Trap*** *as the only event response; if a trap is lost due to a collision or other transmission problem, it will not be re-sent.*

c. Select both **Log** and **Trap** to both log the event occurrence and generate the traps.

If you select neither option, the event's occurrences will neither be logged nor generate traps; unless the event includes an action or a series of actions, this effectively disables the event (since there will be no indication that it has been triggered).

NOTE

The Event Type field in the Advanced Alarm/Event List window will display a value of "none" if neither the Log nor the Trap response has been selected; note, however, that this field does not indicate whether or not an event has been configured to perform an SNMP SET or series of SETs via the Actions MIB.

7. For devices which support the proprietary Actions MIB, an **Actions** button will appear in the Create/Edit Events window; using this feature, you can configure an SNMP SET or series of SETs that will be performed automatically when the event is triggered. See **Adding Actions to an Event**, below, for more information.

8. Click the **Apply** button to set your changes. Note that the window remains open so that you may configure additional new events or modify existing ones; remember, you can double-click on any event in the Events Watch list in the main Alarm/Event window to display its parameters in the Create/Edit Events window (and in the Create/Edit Actions window, if it's open). When you have finished configuring your events, click on the **Cancel** button to close the window.

Adding Actions to an Event

For devices which support the proprietary Actions MIB, selecting the **Actions** button in the Create/Edit Events window opens the Create/Edit Action window (Figure 4-6), which allows you to define an SNMP SET or series of SETs that will be performed automatically when the associated event is triggered.

To add an action or actions to an event:

1. In the Create/Edit Events window, click on the **Actions** button. The Create/Edit Action window, Figure 4-6, will appear.

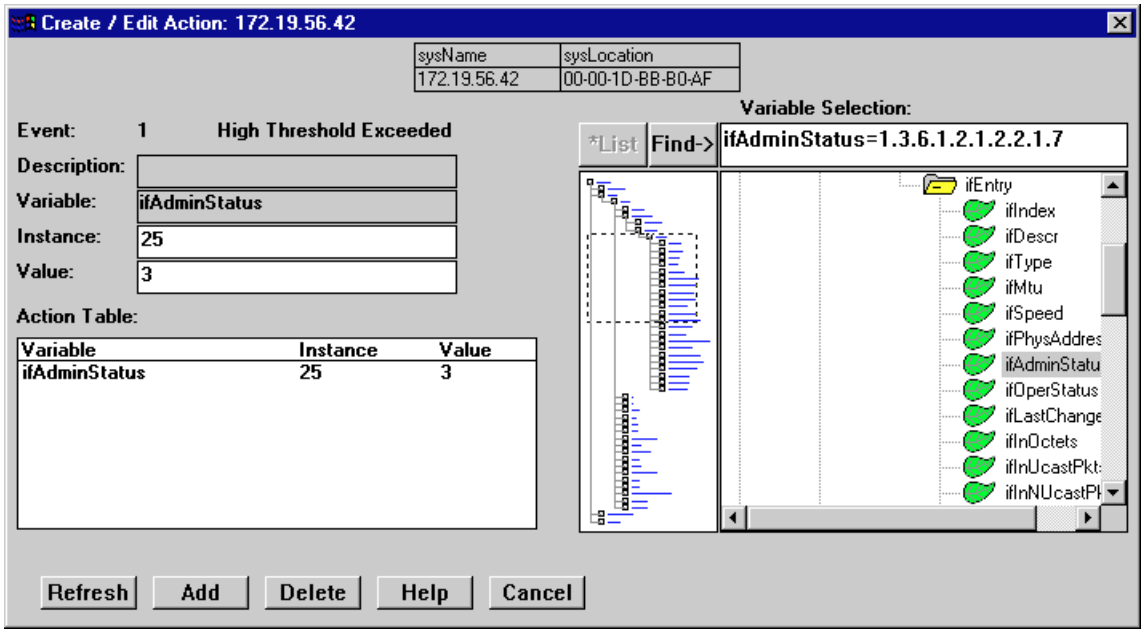
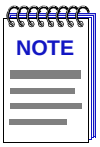


Figure 4-6. The RMON Create/Edit Action Window

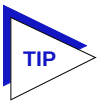


*If no **Actions** button appears in the Create/Edit Events window, the selected MultiSwitch 700 module does not support the Actions MIB. For more information about devices which support this MIB, contact the Global Call Center.*

2. The index number and description of the event with which the action or actions will be associated is displayed in the **Event:** field at the top of the window. Information in this field is not editable; to assign actions to a different event, double-click on the correct event in the Events Watch list; both the Create/Edit Events and Create/Edit Action windows will update accordingly.
3. The **Description** field is not currently editable.
4. To select the **Variable** whose value you wish to SET, use the MIB Tree display provided on the right side of the window. (For more information about how to use the MIB Tools browser, see the ***Tools Guide***.) The display will default to the top of the tree (labeled Internet); there are two ways to locate and/or assign the correct variable:

a. If you know the exact name of the OID value you wish to track (including its capitalization), simply enter the name in the **Variable** field; to verify that you have entered the name correctly, click on the **Find->** button to move the MIB Tree display to that OID. (If MIB Tree display does not adjust to show the OID you've entered, you've entered the name incorrectly; remember, case does count!)

b. Use the scroll bars and click to open the appropriate folders in the MIB Tree display to locate the object you wish to use; click to select it in the panel, and its name will automatically be entered in the **Variable** field.



If you select an invalid OID — that is, one which does not permit write access — the message !!Can't set action on this type!! will be displayed in the Variable field.

If you don't know the exact spelling of the OID you wish to use for your alarm variable, and you can't find it by searching through the tree, use the MIB Tools utility's Find feature to locate the OID and determine its exact spelling (and tree location). For more information on the MIB Tools utility and its Find capabilities, see the **Tools Guide**.

5. Once you have selected the object you wish to set, you must assign the appropriate instance value in the **Instance** field. If you're not sure how the object you wish to set is instanced, you can use the MIB Tools utility (described in the ***Tools Guide***) to query it; all available instances for the object will be displayed.

6. In the **Value** field, enter the value you wish to set for the selected object. Again, if you're not sure what the valid values are for the variable you wish to set, locate the object in the MIB Tools utility and use the **Details** tab to obtain more information.

7. Once you've configured your action, click on the **Add** button; the action will be added to the Action Table list in the lower left corner of the window. Note that the window remains open so that you may configure additional new actions or modify existing ones; selecting on any action in the Action Table will display that action's parameters in the window and make them available for editing. When you have finished configuring your actions, click on the **Cancel** button to close the window.

Note that the Action Table will update automatically each time an action is added or deleted; use the **Refresh** button to update the table at any time.

Deleting an Alarm, Event, or Action

To delete an alarm, event, or action:

1. In the appropriate window, highlight the alarm, event, or action you wish to remove.
2. Click on the **Delete** button to remove. A window will appear asking you to confirm your selection; click on the **OK** button to delete, or on the **Cancel** button to cancel.

When you delete an event, be sure you edit all alarms that were pointing to that event, and assign a new valid event to those thresholds; note, too, that deleting an event automatically deletes its associated actions, as actions cannot exist in the absence of an association with an event.

As a general rule, we recommend that you do *not* delete an alarm or event of which you are not the owner.

Viewing an Advanced Alarm Event Log

To view the log of occurrences for any event:

1. Highlight the event for which you wish to view the log, then click on the **Event Log** button at the bottom of the Advanced Alarm/Event List window; the Event Log window, Figure 4-7, will appear.

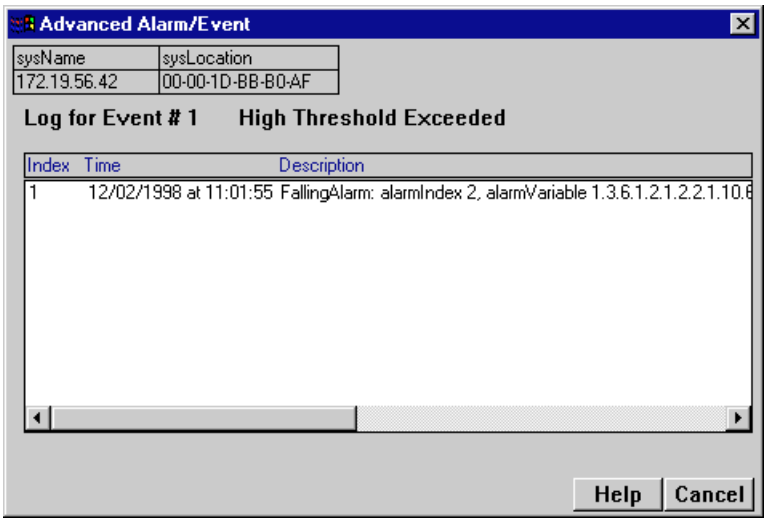


Figure 4-7. The Event Log Window

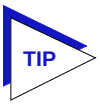
The top portion of the window contains the device information boxes, as well as the event index number and the event description; the log itself includes the following fields:

Index	This uniquely identifies this ***occurrence*** of the event.
Time	Indicates the date and time of each event occurrence.
Description	Provides a detailed description of the alarm that triggered the event: whether it was a rising or falling alarm, the alarm index number, the alarm variable name and object identifier (OID), the alarmSampleType (1=absolute value; 2=delta value), the value that triggered the alarm, the configured threshold that was crossed, and the event description. Use the scroll bar at the bottom of the log to view all the information provided.

Each log will hold only a finite number of entries, which is determined by the resources available on the device; when the log is full, the oldest entries will be replaced by new ones.

How Rising and Falling Thresholds Work

Rising and falling thresholds are intended to be used in pairs, and can be used to provide notification of spikes or drops in a monitored value — either of which can indicate a network problem. To make the best use of this powerful feature, pairs of thresholds should not be set too far apart, or the alarm notification process may be defeated: a built-in hysteresis function designed to limit the generation of events specifies that, once a configured threshold is met or crossed in one direction, no additional events will be generated until the opposite threshold is met or crossed. Therefore, if your threshold pair spans a wide range of values, and network performance is unstable around either threshold, you will only receive one event in response to what may be several dramatic changes in value. To monitor both ends of a wide range of values, set up two pairs of thresholds: one set at the top end of the range, and one at the bottom.



The current version of the Basic Alarms window only allows you to configure a single pair of thresholds for each alarm variable on each interface; be sure to keep this hysteresis function in mind when configuring those threshold values.

Chapter 5

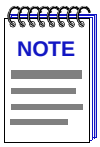
FDDI Management

Concentrator configuration; connection policy; station list; concentrator performance; FDDI statistics; frame translation

The FDDI menu lets you access windows to view a MultiSwitch 700 module's FDDI configuration, connection policy, station list, and performance with respect to each Station Management (SMT) entity present on an installed DELHF-UA modular interface. You can also configure your module's frame translation settings using the Frame Translation window.

The Device View for a MultiSwitch 700 with an installed DELHF-UA will also offer a FDDI Statistics window, which can be launched from the **Device** menu.

SMT provides the system management services for the FDDI protocols, including connection management, node configuration, error recovery, statistics collecting, and management frame encoding. SMT is comprised of various subcomponent functions, including Connection Management (CMT) and Ring Management (RMT); one SMT entity will be present for the ring connected to the DELHF-UA.



The FDDI menu and associated management windows will only appear if you have a DELHF-UA installed in a MultiSwitch 700 module.

Viewing FDDI Information

The windows that provide information about the FDDI ring connected to the MultiSwitch 700 module are:

- **Configuration** — This window displays the current configuration and status of the ring associated with the selected SMT entity.

- **Connection Policy** — This window shows the types of connections between the four FDDI PHY (port) types — A, B, M, and S — that will be allowed by the SMT entity.
- **Station List —** With this window you can see the configuration of the ring on which the SMT entity resides, including number of nodes, node addresses (both Canonical and MAC), node class, and current ring topology.
- **Performance** — This window lets you view the number of frames transmitted and received on the ring as detected by the selected SMT entity, along with error and lost frames, and the number of ring initializations.
- **FDDI Statistics** — This window allows you to view various traffic-related statistics for each SMT entity present on the device.

To access FDDI information (except FDDI Statistics):

1. In the Device View window, click on **FDDI**; drag down to select the SMT entity of interest, then right to reveal the FDDI Information menu (Figure 5-1).

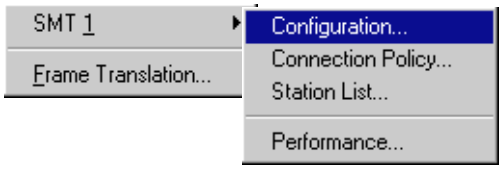
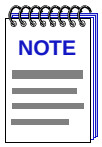


Figure 5-1. The FDDI Menus

2. Select the desired option.



The title bar of each window displays the index number of the SMT entity whose information is being displayed.

To access the FDDI Statistics window:

1. In the Device View window, click on **Device** to display the Device menu.
2. Click on **FDDI Statistics**; **The FDDI Statistics Window**, as shown in Figure 5-6 on page 5-13, will appear.

Configuration

The Concentrator Configuration window, Figure 5-2, informs you about the configuration and operating state of the FDDI ring associated with the selected SMT entity, and displays parameters relating to ring initialization.

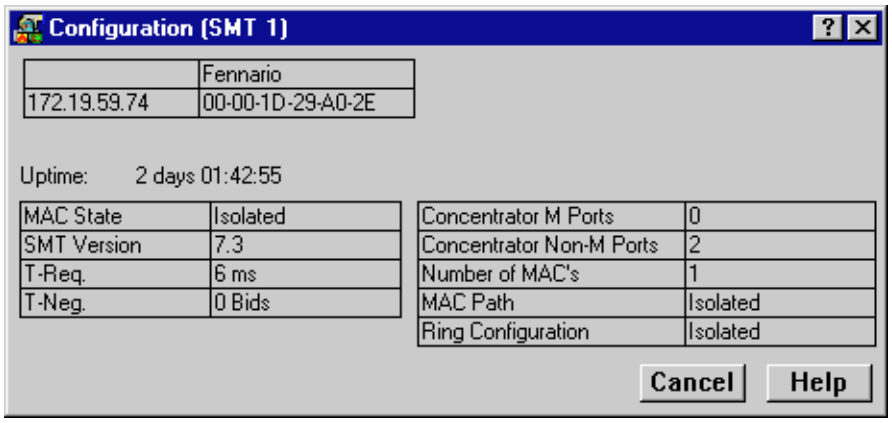


Figure 5-2. The Concentrator Configuration Window

MAC State

This field indicates the current state of the selecting ring's MAC component. (The RMT component of SMT monitors MAC operation and takes actions necessary to aid in achieving an operational ring.) Possible states are:

Not Available	There is no MAC on the FDDI ring associated with the SMT entity.
Ring-Op	The ring is functioning normally. While in this state, the MAC being managed is part of an operational FDDI ring.
Isolated	SMT has just initialized RMT or RMT has entered this state during a path test (trace) after ring beaconing; RMT is not aware of the ring path or state.
Non-Op	The MAC being managed by the selected SMT is participating in ring recovery; the ring is not operational.
Detect	The claim (beacon) process of the FDDI ring protocol has exceeded one second. There may be a problem on the ring; any duplicate address conditions are being detected. In this state, the ring is still alive, but no data is being transmitted.
Non-Op-Dup	The ring is not operational; the address of the MAC under control of the SMT entity has been found to duplicate that of another MAC on the ring. The duplicate address condition prevented ring recovery and initialization after a claim and beacon process. This state

	will not occur unless you are using locally-administered addresses, as factory-set MAC addresses are guaranteed to be unique.
Ring-Op-Dup	The ring is operational; however, the address of the MAC under control of the SMT entity has been found to duplicate that of another MAC on the ring. Corrective actions will be attempted before the duplicate address condition causes ring initialization to fail after the claim and beacon recovery process. Like Non-Op-Dup, this state will not occur unless you are using locally-administered addresses.
Directed	The beacon process did not complete within 7 seconds. The selected SMT has directed the controlled MAC to send beacon frames to notify the other stations that a serious problem exists on the ring, and a Trace state is soon to follow.
Trace	A problem exists on the ring which could not be corrected during the beaconing process, and a Trace has been initiated. During a Trace (or Path Test), the SMT sends a signal that forces its nearest upstream neighbor to remove from the ring and conduct a self-test. If the ring does not recover, each subsequent upstream station will be forced to remove from the ring and conduct self-tests until the problem has been corrected. While the test is being conducted, ring management re-enters the isolated state.

SMT Version

Displays the version number of the Station Management (SMT) entity. SMT provides the system management services for the FDDI protocols, including connection management, node configuration, error recovery, and management frame encoding. SMT frames have a version ID field that identifies the structure of the SMT frame Info field. The version number is included in the SMT frame so that a receiving station can determine whether or not its SMT version is able to communicate with the SMT version of another station. Knowing the version number allows the stations to handle version mismatches. Each FDDI station supports a range of SMT versions. The supported version range is identified within the ietf-fddi MIB by two smtTable attributes: *snmpFddiSMTLoVersionId* and *snmpFddiSMTHiVersionId*. If a received frame is not within the supported version range, the frame is discarded.

T-Req. (Requested Target Token Rotation Time)

The token rotation time bid made by the selected SMT entity during ring initialization. Each station detecting that the ring must be initialized begins a claim token process and issues a stream of Claim Frames, which negotiate the value assigned to the Target Token Rotation Time (TTRT). The information field of these frames contains the issuing station's bid for the value of TTRT. Each claiming station inspects incoming Claim frames (from other issuing stations) and

either continues its own bid (and removes the competing Claim Frame from the ring) or defers (halts transmission of its own bid and repeats the competing bid) according to the following hierarchy of arbitration:

- A Claim Frame with the lowest TTRT bid has precedence.
- If the values of TTRT are equal, the frame with the longest source address (48 vs. 16 bits) has precedence.
- If both TTRT value and source address length are equal, the frame with the highest address has precedence.

The DELHF-UA is shipped with a default T-Req of 6 msec. T-Req is stored within the MIB in units of nanoseconds (one billionth of a second) rather than milliseconds (one thousandth of a second); NetSight Element Manager converts nanoseconds to milliseconds for display purposes. You can use any SNMP Set Request tool to edit the T-Req value; just remember that you must enter your value in nanoseconds, rather than milliseconds.

T-Neg. (Negotiated)

The winning time negotiated in the ring initialization sequence.

Concentrator M Ports

This field displays the number of Master (M) ports on the device that are associated with the selected SMT entity. A Master port is a port that provides a connection for Single Attachment Station (SAS) devices to the FDDI network. The DELHF-UA does not support M ports, so this field will always display 0.

Concentrator Non-M Ports

This field display the number of non-Master ports (A, B, or S ports) on the device that are associated with the selected SMT entity. As each DELHF-UA module has a single A /B port pair supporting a single ring (and, therefore, a single SMT entity), this field will display 1.

Number of MACs

The number of Media Access Control entities present on the device associated with the selected SMT entity. For the DELHF-UA, this number will be 1.

MAC Path

Indicates the configuration of the MAC in respect to the logical ring, as determined by the Connection Management (CMT) portion of SMT. CMT controls the establishment of a media attachment to the FDDI network, the connections with other nodes in the ring, and the internal configuration of the various entities within a node. CMT provides the link confidence test, and specifies a Link Error Monitor (LEM) which monitors active links on a per-link basis to ensure that failing links are detected and, if required, removed from the network. Possible values are:

- **Primary** indicates that the MAC is inserted into the primary path of the currently used FNB ring.

- **Secondary** indicates that the MAC is inserted into the secondary path of the currently used FNB ring.
- **Local** means that the MAC is not inserted into a primary or secondary path of a dual ring, but may be connected to one or more other nodes. This is not a valid value for the DELHF-UA.
- **Isolated** means that the MAC has no connection to the ring or other concentrator ports.
- **Not Available** means that there is no MAC on the FDDI ring associated with the selected SMT entity. Again, this state will not occur for the DELHF-UA.
- **Unknown** means that device firmware cannot determine the MAC path.
- **?** indicates that NetSight Element Manager cannot determine the MAC path for the selected ring.

Ring Configuration

The current configuration of the MAC and physical layers of the A and B ports.

Connection Policy

The SMT Connection Policy of an FDDI concentrator determines which types of connections are allowed among the four FDDI port types: A, B, M (Master), and S (Slave). FDDI protocol forbids Master—>Master connections; all other connection types are legal, although some are considered to be undesirable.

The Connection Policy window, Figure 5-3, lists potential connection types in a "Reject X-Y" format, where **X** represents a port on the DELHF-UA, and **Y** represents the attaching node. An **X** in the checkbox next to a Connection Policy indicates that the connection has been disallowed.

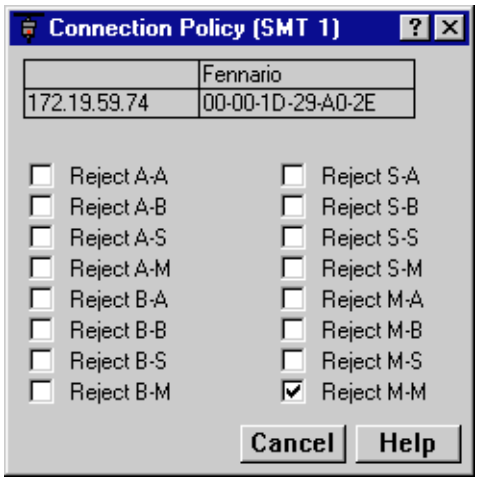


Figure 5-3. The Connection Policy Window

The following table summarizes the FDDI connection rules:

Table 5-1. FDDI Connection Rules

	A	B	S	M
A	V, U	V	V, U	V, P
B	V	V, U	V, U	V, P
S	V, U	V, U	V	V
M	V	V	V	X

V —valid connection
X —illegal connection
U —undesirable (but legal) connection; this requires that SMT is notified.
P —valid, but when both A and B are connected to M ports (a dual-homing configuration), only the B connection is used.

Though technically legal under FDDI connection rules, undesirable connections will cause a twisted or wrapped ring.

Each SMT entity maintains its own connection policy; however, when two interfaces attempt to connect, their combined established connection policies dictate the connections that will be allowed. In an attempted connection between two nodes, the most lenient policy will determine whether the connection (as long as it is legal) can be made. For example, if two FDDI nodes attempt an A—>A connection, and this connection is not allowed at one FDDI node but allowed at the other, the connection would be accepted. If the connection policy at both nodes disallows the connection, the connection will be rejected.

This is a read-only window; you currently cannot edit the DELHF-UA's connection policy via NetSight Element Manager.

You can use any SNMP Set Request or MIB tool to edit the Connection Policy for your device by setting the fddimibSMTConnectionPolicy MIB OID (part of the MIBII FDDI Transmission MIB (RFC1512). fddimibSMTConnectionPolicy is simply a 16-bit integer value (ranging from 32768 to 65535) that corresponds to the connection policy (in the "Reject X-Y" format, where X represents a port on the FDDI Switch Module, and Y represents the attaching node).

To set the connection policy for the device, total the bit values corresponding to the desired connection policy according to the table below, and then use your SNMP Set Request or Mib tool to set the value for the appropriate SMT index. For example, to set a connection policy that disallowed the undesirable A-A or B-B connections you would set the fddimibSMTConnectionPolicy MIB OID to 32,801: 32,768 (reject M-M, required) + 32 (reject B-B) + 1 (reject A-A).

Policy	*Power*
reject A-A	2^0 *(1)*
reject A-B	2^1 *(2)*
reject A-S	2^2 *(4)*
reject A-M	2^3 *(8)*
reject B-A	2^4 *(16)*
reject B-B	2^5 *(32)*
reject B-S	2^6 *(64)*
reject B-M	2^7 *(128)*
reject S-A	2^8 *(256)*
reject S-B	2^9 *(512)*
reject S-S	2^{10} *(1,024)*
reject S-M	2^{11} *(2,048)*
reject M-A	2^{12} *(4,096)*
reject M-B	2^{13} *(8,192)*
reject M-S	2^{14} *(16,384)*
reject M-M	2^{15} *(32,768 — a permanently set value for this bit)*

Station List

The Station List illustrates the configuration of the ring associated with the currently selected SMT entity, including number of nodes on the ring, node addresses (both Canonical and MAC), node class, and ring topology.

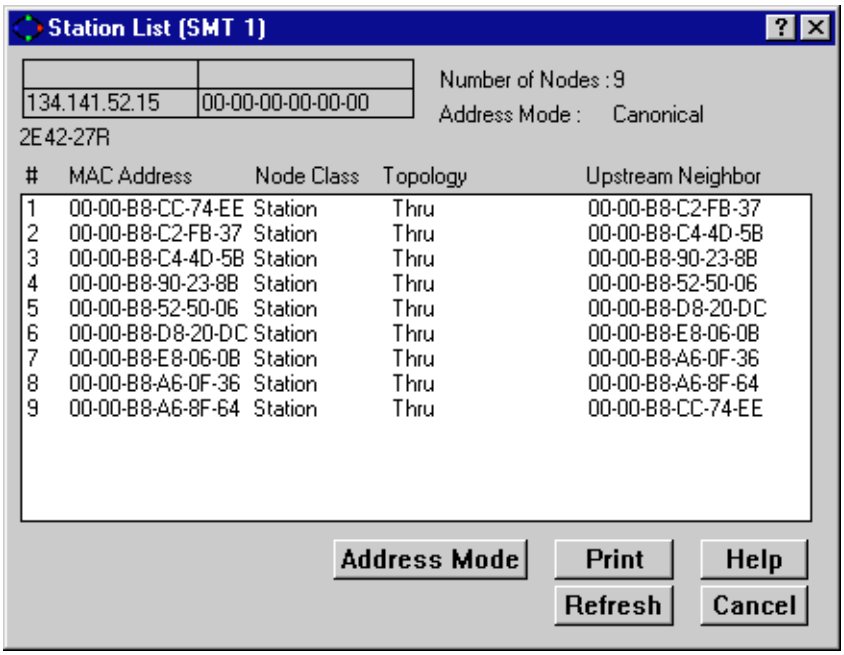


Figure 5-4. The Station List Window

The Station List provides the following information about the ring with which the SMT is currently associated:

Number of Nodes

The number of stations inserted into the FDDI ring with which the SMT entity is currently associated.

Address Mode

Displays the current mode being used to display the addresses of the devices in the Station List. The two possible modes are Canonical (FDDI) or MAC (Ethernet).

To change the current Address Mode, click on the **Address Mode** button at the bottom of the window. The current address mode will change in the Address Mode field and the Stations panel.

Stations Panel

The Stations Panel displays a list of the stations on the ring to which the selected SMT is connected, in ring sequence from the MAC, along with each station's node class and current topology. If the number of nodes exceeds the panel size, scroll bars will appear in the list box that will allow you to scroll through the station list to view the node of interest

Information provided in the Stations Panel includes:

#
An index number assigned to each station that indicates its position on the ring in relation to the monitored SMT's MAC address. The monitored SMT's MAC is always the first entry (1) in the station list.

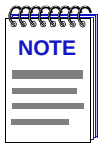
MAC Address
Displays the 48-bit hardware address —þused for universal address assignment —þof the node inserted into the ring. These addresses are hardcoded into the device, and are not configurable. The address will appear in Canonical or MAC format, as currently selected.

Node Class
Displays the type of ring device. Possible values are:

Station	Indicates an FDDI node capable of transmitting, receiving, and repeating data.
Concentrator	Indicates an FDDI node that provides attachment points to the ring for stations that are not directly connected to the dual ring.

Topology
Indicates the node's MAC configuration topology.

Upstream Neighbor
Displays the hardware address (in Canonical or MAC format, as currently selected) of each node's upstream neighbor.



The information displayed in the Station List is static once the window is opened; for updated information, click **Refresh**.

Performance

The Concentrator Performance window, Figure 5-5, provides graphical and numeric performance statistics for the selected SMT entity, including transmit frames, receive frames, frame errors, lost frames, and ring ops.

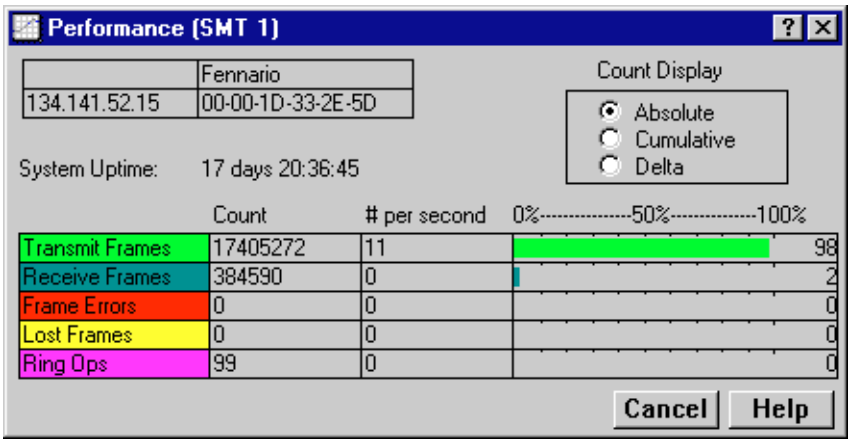


Figure 5-5. The Concentrator Performance Window

Statistics are displayed in three ways:

- By count (i.e., the number detected of each for the selected interval).
- By rate (i.e., the number of each per second, as averaged over the selected interval).
- Graphically, as a percentage of each with respect to total network load processed by the DELHF-UA interface during the last interval (e.g., a transmit frames rate of 75% during a delta interval indicates that of all frames *processed* by the selected interface, 75% were *transmitted* by that interface).

You can view the concentrator performance for three different intervals:

- **Absolute** — Counts recorded since the MultiSwitch 700 module was last started.
- **Cumulative** — Counts recorded since the Concentrator Performance window was opened.
- **Delta** — Counts recorded during a single polling interval (refer to the ***User's Guide*** for information on setting the polling interval).

To change the interval, click to select the desired radio button in the **Count Display** panel in the top right hand corner of the window.

Available statistics are:

Transmit Frames
The number of frames transmitted by the MAC associated with the SMT during the chosen interval.

Receive Frames
The number of frames received by the MAC associated with the SMT during the chosen interval.

Frame Errors
The number of error frames detected by the MAC associated with the SMT during the chosen interval that had not been detected previously by other stations. Error frames may include frames with an invalid Frame Check Sequence (FCS), with data length errors, or with internal errors that prevent the MAC from transferring the frame to the Logical Link Control (LLC) layer.

Lost Frames
The number of frames detected by the MAC associated with the SMT during the chosen interval that have an unknown error, so their validity is in doubt. When the MAC encounters a frame of this type, it increments the Lost Frame counter and strips the remainder of the frame from the ring, replacing it with idle symbols.

Ring Ops
The number of times the ring has entered the "Ring Operational" state from the "Ring Not Operational" state during the selected interval. This counter updates when the MAC informs Station Management (SMT) of a change in Ring Operation status.

FDDI Statistics

The FDDI Statistics window displays traffic statistics for the DELHF-UA's SMT entity, including the number of frames and kilobytes per second (averaged over a defined poll rate), the peak number of kilobytes per second, and the module's bandwidth utilization (expressed as a percentage) for the current poll interval.

To access the FDDI Statistics window:

1. In the Device View window, click on **Device** to display the Device menu.
2. Select **FDDI Statistics**. The FDDI Statistics window (Figure 5-6) will appear.

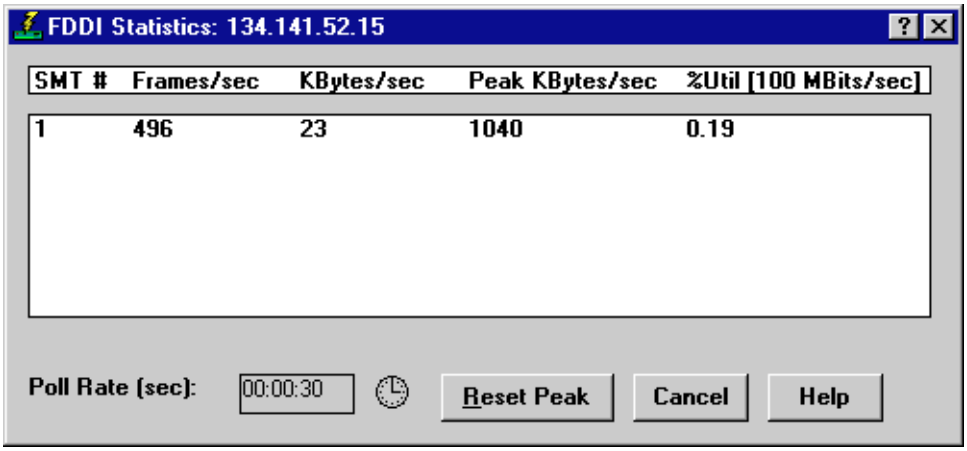


Figure 5-6. The FDDI Statistics Window

The FDDI Statistics window displays the following information for the module:

SMT#
This field displays the index number of Station Management (SMT) entity for the DELHF-UA.

Frames/sec
The number of frames / second (averaged over the specified poll interval) transmitted by the indicated SMT.

KBytes/sec
The number of kilobytes / second (averaged over the specified poll interval) transmitted by the indicated SMT.

Peak KBytes/sec
The peak number of kilobytes / second transmitted by the indicated SMT, as detected over all polling intervals since monitoring began (i.e., since the FDDI Statistics window was first opened).

%Util
The percentage of utilization of available bandwidth by the indicated SMT over the current poll interval; the percentage is calculated by dividing the actual number of transmitted bytes / sec into the maximum number of bytes / sec that could be transmitted (125,000,000 bytes / sec potential on a 100 Megabit / second ring).

Setting the FDDI Statistics Poll Rate

To set the FDDI Statistics poll rate:

1. Click on the clock symbol ( ) next to the **Poll Rate (sec)** text box. The New Timer Interval text box, Figure 5-7, will appear.

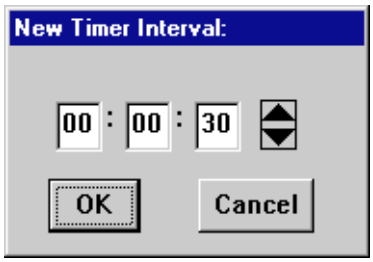


Figure 5-7. New Timer Interval Text Box

2. Using the mouse, click to highlight the **hour** field in the New Timer Interval text box.
3. Using the arrow keys to the right of the text box, scroll to change the hour, as desired. Notice that the time is given in a 24-hour hh:mm:ss format.
4. Using steps 2 and 3, continue to change the **minutes** and **seconds** fields, as desired.
5. Click on **OK** when you are finished entering new information. The new Poll Rate you have set is now entered.

The FDDI Statistics window will refresh, and the new time interval will take effect immediately.

Configuring FDDI Frame Translation Settings

The DELHF-UA interface must be configured to translate packets from an FDDI frame format to an Ethernet frame format (and vice versa) when bridging packets between FDDI and Ethernet networks. The Frame Translation window lets you set the parameters for frame translation.

To access the FDDI Translation window (Figure 5-8):

1. In the Device View window, click on **FDDI** to display the FDDI menu.
2. Select **Frame Translation;** the Frame Translation window, as shown in Figure 5-8, will appear.

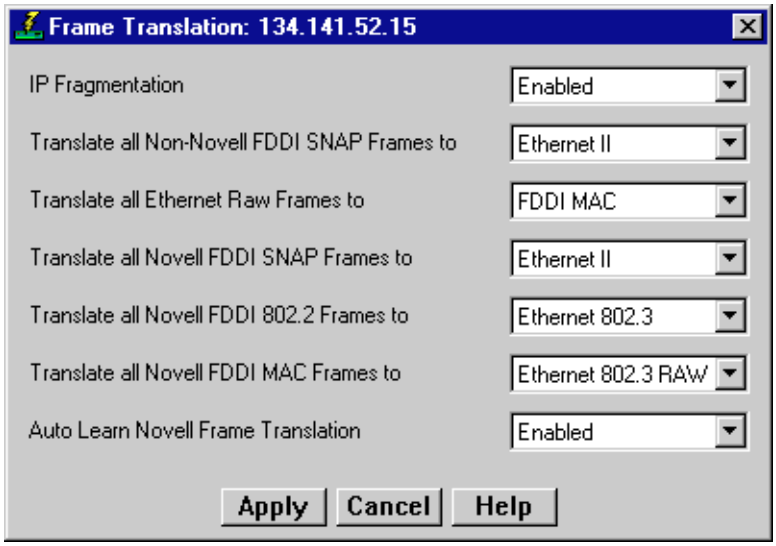


Figure 5-8. The Frame Translation Window

Information about Ethernet and FDDI Frame Types

There are four frame types which can be transmitted on an IEEE 802.3/Ethernet network – **Ethernet II**, **Ethernet 802.2**, **Ethernet 802.3** (or Raw Ethernet), and **Ethernet SNAP**; there two frame types which can be transmitted on an FDDI network: **FDDI 802.2** and **FDDI SNAP**. Each of these frame types is described in more detail in the sections that follow. Bridges connecting IEEE 802.3/Ethernet LANs to an FDDI ring have to provide frame translation, as there are addressing and frame format differences between the two network topology types.

For an Ethernet frame format to be forwarded onto an FDDI network, the Length (IEEE 802/SNAP) or Type (Ethernet II) field must be removed (along with any frame padding), an FDDI Frame Control field must be added, the bit-order of the address fields must be reversed, and the frame's CRC field must be recomputed.

In most instances, the IEEE 802.3/Ethernet frame format is translated automatically into the appropriately corresponding FDDI frame format. Ethernet 802.2 frames are translated to FDDI 802.2 frames; Ethernet II frames are translated to FDDI SNAP frames; non-AppleTalk Ethernet SNAP frames are translated to FDDI SNAP frames; and AppleTalk Ethernet SNAP frames are translated to FDDI SNAP frames (AppleTalk format).

However, because Ethernet Raw frames do not have a Type or Length field, and can't be automatically translated onto an FDDI network, you must select the appropriate translation method to an FDDI frame format (for transmitting to FDDI stations or for bridging back to an Ethernet network).

If the frame is exiting the FDDI ring through another FDDI/Ethernet bridge, the FDDI frame must be converted back into an IEEE 802.3/Ethernet frame. As there are four potential Ethernet frame types to which the two FDDI frame types can be translated, you must determine which translation options you want in effect — depending on which network protocols and applications are being run on the destination network.

In addition, there are frame size differences between FDDI (which allows a maximum frame size of 4500 bytes) and Ethernet frames (1518 byte maximum, excluding preamble), so FDDI frames may need to be fragmented before being bridged onto an Ethernet network.

The Frame Translation window lets you set the parameters for frame translation and fragmentation when Ethernet traffic needs to traverse an FDDI ring. The frame types that you select for translation will depend on which higher-layer communications protocols and software you are running on the network segments connected to your Ethernet-to-FDDI bridge. Each frame type and its usage is described below.

Ethernet Frames

The DELHF-UA supports translation of the following four Ethernet frame types:

Ethernet II

Ethernet II is the Novell NetWare designation for the basic Ethernet frame type (also commonly referred to as Ethernet or Ethernet DIX). This frame format has an Ethernet II MAC header with a two byte Ethernet **Type** field. The Type field contains a protocol ID which indicates the upper layer protocol (e.g., XNS, DECnet, TCP/IP, etc.) used in the Data field of the packet. Most current transmission protocols, including TCP/IP, use the Ethernet II frame format, as do networks running Apple's AppleTalk 1 protocol and Digital's DECnet™ protocol.

Note that the Type field of an Ethernet II frame will always have a decimal value greater than 1500, so that it can be differentiated from the Length field of Ethernet 802.2 frames (described below).

Ethernet 802.2

The Ethernet 802.2 frame format is the IEEE 802.3 formalization of the original Ethernet frame format. This frame format is similar to the Ethernet II frame format, except that the two byte Type field is eliminated and replaced with a two byte **Length** field, and an 802.2 LLC header is encapsulated within the 802.3 frame. This LLC header contains the destination and source addressing information for the LLC frame (DSAP and SSAP), and a one byte Control field (the LSAP – or LLC Service Access Point value) which provides the frame's protocol ID. Ethernet 802.2 packets are differentiated from Ethernet II packets because the Length field will always have a decimal value of 1500 or less (since the data field in Ethernet frames cannot be greater than 1500 bytes), and the Ethernet II Type field will always be greater than 1500 decimal.

This is the default frame type for Novell NetWare software version 3.12 and beyond; it is also used for OSI packets on IEEE 802.x LAN networks.

Ethernet 802.3 (Ethernet Raw)

The Ethernet 802.3 frame format has an 802.3 MAC layer header (as do Ethernet 802.2 frames); however, it does not contain an 802.2 LLC header. Instead, Novell IPX is fixed within the packet as the network layer protocol. This frame type – also known as **Raw 802.3** – is the default frame type for Novell NetWare software before version 3.11. Since these frames do not carry the 802.2 header, they do not conform to the IEEE 802.3 specification. If you are using the Ethernet 802.3 Raw frame format, you should consider upgrading your Novell NetWare software to ensure interoperability with other communications protocols (unless your current network is not likely to be upgraded, and has no interoperability problems).

Note that IPX packets with checksums which provide data integrity (a feature of newer Novell NetWare releases) cannot be transmitted on Ethernet 802.3 networks. Note also that a single Ethernet can carry both Ethernet 802.3 and Ethernet 802.2 traffic simultaneously. The Novell server software will treat the two frame types as two logical networks (and function as an IPX router between the two networks).

Ethernet SNAP

To allow for proprietary protocols, such as IBM's SNA protocol, the **Ethernet** SNAP frame was created. This frame format extended the Ethernet 802.2 packet by improving the frame's byte alignment, and by allowing further protocol identification than the one byte LSAP protocol identifier of Ethernet 802.2 frames (which is reserved for standard protocols). Ethernet SNAP packets have an LSAP protocol ID of hex AA, indicating that they contain a **SNAP** (Subnetwork Access Protocol) packet. A SNAP packet, encapsulated within the Ethernet 802.2 packet, has a five byte SNAP header which is simply a five byte protocol identifier. The first three bytes of the header indicate the Organizationally Unique Identifier (OUI) – or the authority assigning the protocol ID – and the last two bytes indicate the protocol according to that authority. Note that for most protocols, the OUI is 0-0-0, and the type identifier is the standard Ethernet protocol ID. Although most Ethernet transport protocols use the Ethernet II frame format, the AppleTalk II protocol uses Ethernet SNAP (AppleTalk has its own unique OUI).

FDDI Frames

There are two legal FDDI data frame types:

FDDI 802.2

The FDDI 802.2 frame type has two headers: the FDDI header (which includes the Frame Control field that indicates the class of frame, length of the address field, and the type of FDDI frame), and the 802.2 header.

FDDI SNAP

The FDDI SNAP frame type has an FDDI header with a Frame Control field that provides FDDI framing information, and the 802.2 LLC header with FDDI Frame Control, a SNAP LSAP identifier, and a five byte protocol identifier.

There is no FDDI equivalent for Ethernet 802.3 Raw frames or Ethernet II frames. Ethernet / FDDI bridges will automatically translate Ethernet II frames into FDDI SNAP frames, by identifying it as a SNAP frame in the LLC header, and inserting a SNAP header with the Ethernet Type field.

By default, Ethernet-to- FDDI bridges will translate an 802.3 Raw frame into an **FDDI MAC** frame – although you can use the FDDI Frame Translation window to alter the default translation. The FDDI MAC frame is an FDDI frame type that is defined for internal use by the MAC layer, and which is not passed to higher layer communications protocols on the datalink layer. Any 802.3 Raw frame translated into FDDI MAC will be recognized as such by many other Ethernet / FDDI bridges inserted in the ring, and will be forwarded onto the target Ethernet segment as an 802.3 Raw frame.

FDDI Frame Translation Options

The FDDI Translation window lets you select which translation methods you want enforced when translating frames from an FDDI frame format into an Ethernet frame format, and when translating Ethernet Raw frames into FDDI frames. It also lets you choose whether to allow fragmentation of IP datagrams into smaller datagrams, and enable or disable the Auto Learn Novell Frame Translation option.

To set frame translation parameters:

1. Click on the selection boxes of interest (described below), and drag to select the desired translation options.
2. Click **Apply** to save your new frame translation settings at the device, or click **Cancel** to restore the last saved options.

IP Fragmentation

The IP Fragmentation selection box lets you specify frame fragmentation parameters. FDDI traffic may need to be split, or fragmented, into two, three, or four smaller frames to be successfully transmitted on an Ethernet network. For fragmentation to be allowed, the frame must be an FDDI SNAP frame with an OUI of 00-00-00 (indicating TCP / IP) and an IP protocol type identifier (08-00). Possible options are **Enabled** (allow IP fragmentation – the default) or **Disabled** (prevent IP fragmentation, and discard frames over 1518 bytes).

Translate all Non-Novell FDDI SNAP frames to

This selection box lets you set the translation parameters for non-Novell FDDI SNAP frames. Possible options are **Ethernet II** (the default, which you should use when bridging to most TCP / IP networks) or **Ethernet SNAP** (which you should use when bridging to an AppleTalk environment on Ethernet).

Translate all Ethernet Raw frames to

This selection box lets you set the translation parameters for Ethernet Raw (Ethernet 802.3) packets. Ethernet Raw frames are used on networks running the IPX protocol on Novell NetWare versions prior to 3.12. Possible options are **FDDI 802.2**, **FDDI SNAP** (generally used when bridging to an AppleTalk environment on an FDDI ring), or **FDDI MAC** (the default option, which translates the frame into an FDDI MAC frame – which will not recognized as a data frame on an FDDI ring, but will be recognized by an Ethernet / FDDI bridge).

Translate all Novell FDDI SNAP frames to

This selection box lets you set the translation parameters for Novell IPX FDDI SNAP frames. Possible options are **Ethernet II** (default, for most TCP / IP traffic), **Ethernet SNAP** (AppleTalk networks), **Ethernet 802.3** (some NetWare 3.12+ or other networks running an ISO / OSI protocol stack), or **Ethernet 802.3 Raw** (NetWare 3.11 and earlier networks).

Translate all Novell FDDI 802.2 frames to

This selection box lets you set the translation parameters for Novell IPX FDDI 802.2 frames. Possible options are **Ethernet II**, **Ethernet SNAP**, **Ethernet 802.3** (default), or **Ethernet 802.3 Raw**.

Translate all Novell FDDI MAC frames to

This selection box lets you set the translation parameters for Novell IPX FDDI MAC frames (i.e., received from a NetWare 3.11 or earlier network, and translated into FDDI MAC frames). Possible options are **Ethernet II** (most TCP / IP networks), **Ethernet SNAP** (AppleTalk Networks), **Ethernet 802.3** (some NetWare 3.12+ and other networks running an ISO / OSI protocol stack), or **Ethernet 802.3 Raw** (default – NetWare 3.11 or earlier networks).

Auto Learn Novell Frame Translation

Some FDDI / Ethernet bridges can automatically learn the appropriate frame translation type by the source address received at the Ethernet interface. If this option is enabled, Novell IPX frames destined to a previously learned source address will be translated to the appropriate frame type for that address (as determined by its previously transmitted frames). If the destination address is unknown, the default frame translation will be used for the frame. Possible options are **Enabled** or **Disabled**.

Chapter 6

ATM Configuration

Viewing connection data; configuring Permanent Virtual Circuits (PVCs); adding and deleting connection entries

The ATM interface provided by the DELHA-UA module provides the connectivity that allows you to merge ATM network segments with traditional LAN technologies via the DLM6C-AA MultiSwitch 700 chassis backplane. Current versions of DELHA-UA firmware use 802.3 VC-based multiplexing for bridging protocols to move PVC traffic between the ATM front panel connection and the switching backplane; future versions will add support for ATM Forum LAN Emulation.

An ATM network uses two types of virtual channels, or circuits: Switched Virtual Circuits, or SVCs, and Permanent Virtual Circuits, or PVCs. SVCs are created and dismantled dynamically on an as-needed basis, and require no management definition; PVCs, however, must be manually configured. The Current ATM Connections window provides the means for accomplishing these configurations.

Accessing the ATM Connections Window

To access the ATM Connections window from the Device View:

1. Click on **Device** on the Device View menu bar to access the Device menu.
2. Select **ATM Connections**. The Current ATM Connections window, Figure 6-1, will appear.

TIP

*The **ATM Connections** option will only be available when at least one DELHA-UA is installed in the module.*

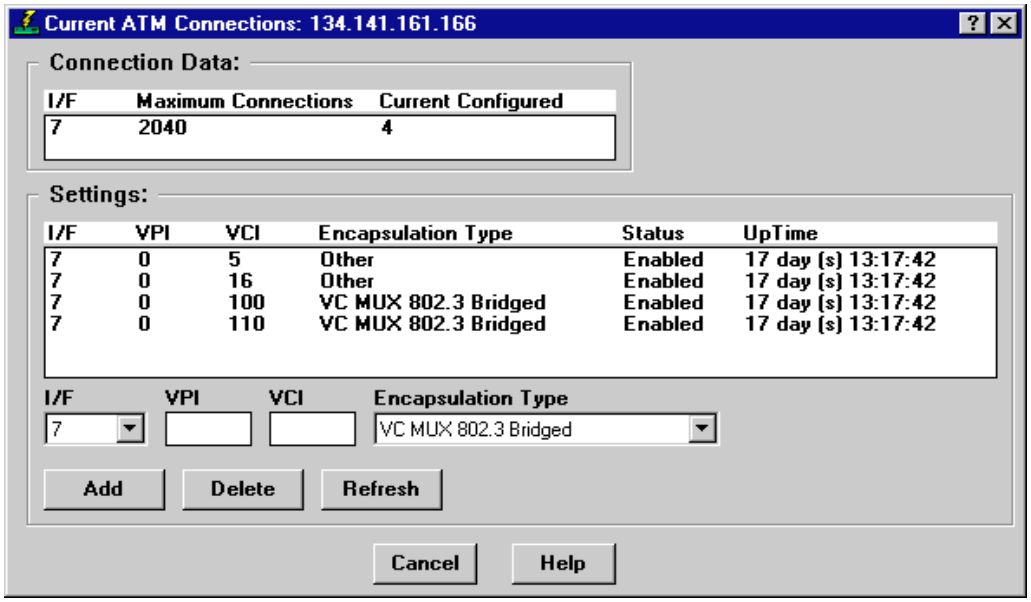


Figure 6-1. The Current ATM Connections Window

The Current ATM Connections window provides the following information about the device's ATM connections:

Connection Data

The Connection Data fields provide the following information about each ATM interface available on the device:

I/F	Displays the index number assigned to each DELHA-UA interface installed in a MultiSwitch 700 module.
Maximum Allowed	Displays the maximum number of connections allowed by current device firmware.
Current Configured	Displays the number of Permanent Virtual Circuits, or PVCs, currently configured.

Settings

The Settings portion of the window contains a list box which displays information about each of the currently configured PVCs, as well as the fields used to configure new connections:

I/F	The device interface on which the PVC was configured.
VPI	Displays the Virtual Path Identifier assigned to the connection; current versions of DELHA-UA firmware allow values from 0-3. Virtual Path Identifiers are used to group virtual connections, allowing for channel trunking between ATM switches. Each VPI can be configured to carry many different channels (designated by VCIs) between two points.
VCI	Displays the Virtual Channel Identifier assigned to the connection; allowable values are 0-1023 *for each VPI*. Each assigned VCI must be unique within its defined VPI: for example, you can assign a VCI of 14 as many as four times: once with a VPI of 0, once with a VPI of 1, and so on. Remember, it is the combined VPI and VCI designations assigned to a channel that creates the grouping of virtual connections.
Encapsulation Type	Displays the method used to encapsulate LAN packets on the selected circuit. Current versions of DELHA-UA firmware use 802.3 VC-based multiplexing for bridging protocols (designated VC MUX 802.3 Bridged); future versions will add support for ATM Forum LAN Emulation. You may also see some connections assigned a type of “other”; these are default connections that cannot be modified or deleted.
Status	Displays the current administrative status of the connection: enabled or disabled. In current versions of firmware, all connections are enabled by default, and cannot be disabled.
UpTime	The length of time the selected connection has been enabled.

Add

Selecting the **Add** button either adds a new connection or modifies an existing one, using the parameters entered in the fields below the list box. A confirmation window will appear for both additions and modifications.

Delete

Selecting the **Delete** button deletes the selected connection; a confirmation window requires that you confirm the deletion.

Refresh
Selecting the **Refresh** button refreshes the connection information displayed in the window.

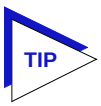
Configuring Connections

You can add a new connection or delete an existing connection as described in the following sections.

Adding a New Connection

To configure new Permanent Virtual Circuits (PVCs), enter the following information in the text fields which appear just below the connections list box:

1. In the **I/F** text box, click on the down-arrow to the right of the text field, and drag down to select the interface for which you wish to configure a connection. All available ATM interfaces will be listed in this menu.
2. In the **VPI** text box, enter the Virtual Path Identifier you wish to assign to this connection. Allowable values are 0 to 3; remember, the VPI you assign will be used to group virtual connections, allowing for channel trunking between ATM switches.
3. In the **VCI** text box, enter the Virtual Channel Identifier you wish to assign to this connection. Allowable values are 0 to 1023 *for each VPI*. For example, you could assign the same channel identifier — say, 25 — as many as four times: once with a VPI of 0, once with a VPI of 1, and so on. Again, remember that it is the combination of VPI and VCI that will be used to direct cells through the intermediate switches between the source and destination.
4. In the **Encapsulation Type** field, click on the down arrow located to the right of the field, and drag down to select the desired encapsulation type. Current versions of DELHA-UA firmware use 802.3 VC-based multiplexing for bridging protocols (designated VC MUX 802.3 Bridged); future versions will add support for additional encapsulation methods.



Selecting any of the other encapsulation types listed in the field's menu will cause a "Set Failed" error when you attempt to add the new connection.

5. Click the **Add** button to add the new permanent circuit to the ATM interface. The circuit is automatically enabled, and will remain in place until it is manually removed.

Deleting a Connection

To delete an existing PVC:

1. In the connections list box, click to select the connection you wish to delete.
2. Click on the **Delete** button. A confirmation window will appear, listing the parameters assigned to the connection and asking you to verify that you wish to delete it. Click on the **OK** button to confirm your selection, or on the **Cancel** button to undo it.

Chapter 7

WAN Configuration

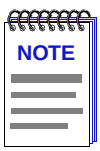
The DELHW-UA and its port interface modules; WAN redundancy; the WAN Logical View; changing WAN Logical settings

The DELHW-UA Wide Area Networking (WAN) modular interface available for the DLE32-MA, DLE33-MA, and other MultiSwitch 700 modules provides LAN-to-WAN switching for the MultiSwitch 700 chassis. It supports IP and IPX bridging or routing services — including IP RIP — and multiple WAN connectivity options via two port interface module slots.

About the DELHW-UA

Unlike other modular interfaces designed for the MultiSwitch 700 boards, the DELHW-UA module functions as an independent intelligent device with its own IP address. As such, it must be managed separately from the MultiSwitch 700 chassis and the board on which it is installed. This chapter provides information on configuring and managing the WAN capabilities of the various port modules available for the DELHW-UA.

The WAN functionality described in this chapter is accessed from the DELHW-UA's Device View. See **The DELHW-UA Device View**, on page 2-75 of Chapter 2, **The MultiSwitch 700 Device View**, for instructions on launching the DELHW-UA Device View. Other DELHW-UA Device View functions, such as finding a source address and changing the device time and date, are also described there.



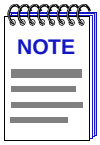
A Windows 95- and NT-based utility called QuickSET for the DELHW-UA was shipped with your DELHW-UA. This program is designed for point-and-click installation and set-up of DELHW-UA devices. Currently, QuickSET should be used to configure all port interface module settings and routing/bridging protocols, including those port interface modules not currently supported by NetSight Element Manager. See your QuickSET documentation for more information. Future releases of NetSight Element Manager will support the DELHW-UA more comprehensively.

Port interface modules available for the DELHW-UA include:

DELDS-UI	DDS is Digital Data Services, a digital network that supports data rates of 56Kbps or 64Kbps. The DDS service provides users with dedicated, two-way simultaneous transmission capabilities operating at transfer rates up to 64 Kbps. This port module comes with a built-in CSU / DSU.
DELDI-UI	The DI (Drop-and-Insert) port interface module provides a T1 interface through a front-panel RJ45 port and includes a built-in CSU / DSU for direct connection to a T1 line. The DELDI-UI provides Full T1 or Fractional T1 using 56 or 64 Kbps Time Slots. It also provides a second Drop-and-Insert interface that allows more than one device, such as a PBX, to share a single T1 connection.
DELE1-UI	This port interface module provides an E1 interface through a front-panel RJ-45 port and includes a built-in CSU / DSU for direct connection to an E1 line. It provides Full E1 or Fractional E1 using 56 or 64 Kbps Time Slots with a total throughput of up to 2 Mbps. Time Division Multiplexing (TDM) allows for the channelization of up to 31 links of a single physical interface.
DELST-UI	This port interface module provides an ISDN 128 Kbps Basic Rate Interface (BRI) and is designed for an ISDN back-up link for a frame relay or leased line. In the United States and Canada, Network Terminator equipment (NT1) is required to provide an interface between the DELST-UI and the ISDN line.
DELSY-UI	Provides a synchronous serial connection of up to 2.048 Mbps to external communications equipment (an external CSU / DSU is required). An external CSU / DSU is required; the following electrical interfaces are supported (consult your hardware documentation for cable pinout information): EIA-RS449 V.35 EIA-RS232D X.21 EIA-RS530 EIA-530A RS530 ALT A RS530A ALT A
DELT1-UI	Provides a T1 interface through a front-panel RJ45 port and includes a built-in CSU / DSU for direct connection to a T1 line. The DELT1-UI provides both Full T1 or Fractional T1 using 56 or 64 Kbps Time Slots, with a total

	throughput of up to 1.544 Mbps. Time Division Multiplexing (TDM) allows for channelization of up to 24 links over a single physical T1/FT1 interface.
DELTD-UI	This port interface module provides both a T1 and DDS interface that allows you to easily switch between the two interfaces by changing the physical cabling and reconfiguring the desired interface with either QuickSET for the DELHW-UA or NetSight Element Manager.

For more information on these port modules, consult the appropriate hardware documentation or your QuickSET for the DELHW-UA documentation.



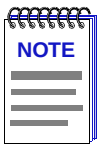
The DELDI-UI and DELE1-UI are not supported by NetSight Element Manager at the time of this release. To configure these port interface modules, use the QuickSET for the DELHW-UA application that was shipped with your device. See your QuickSET documentation for more information.

See **The WAN Logical View** on page 7-4 for details on accessing the WAN Logical View window through the DELHW-UA Chassis View.

WAN Redundancy

For a redundant wide-area connection, one of the WAN interfaces on your DELHW-UA can be configured as a primary link, with the other interface designated as the backup. If the primary link should fail for some reason, the other WAN interface will take over as the wide area link until the primary is restored.

When a DELST-UI is installed as the backup interface, that connection will activate and provide an ISDN connection to the wide area network, if the primary WAN link fails. The ISDN WPIM can also provide backup for single or multiple Data Link Connection Interfaces (DLCIs). If a leased line loses a DLCI or a remote office, for example, the DELST-UI will restore a 64K connection for that site while the rest of the connections remain on the leased line. For more information on WAN redundancy and the DELST-UI, consult your QuickSET documentation or your hardware documentation.



The DELST-UI is designed for WAN ISDN redundancy only and is not intended to be used for a primary WAN connection at this time.

The WAN Logical View

The WAN Logical View window displays information about the interfaces that are part of your physical port. The windows are identical for T1 and Synchronous ports. The number of entries is dependent on the type of port. The T1 port, for example, will have 24 entries.

To access the WAN Logical View window from the DELHW-UA Chassis View:

1. Click on **Device** on the Chassis View menu bar; the device menu will appear.
2. Click on **WAN Status** and then select **Logical View**. The WAN Logical View window, Figure 7-1, will appear.

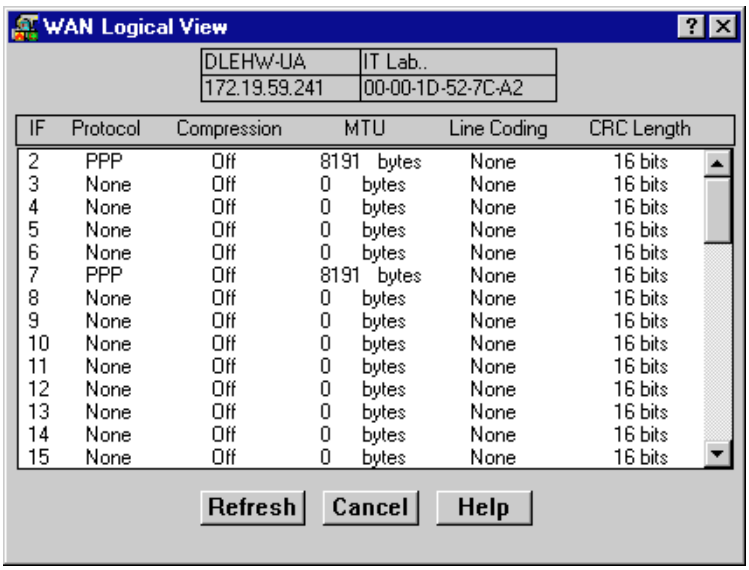


Figure 7-1. The WAN Logical View Window

NOTE

*The information in this window is static; use the **Refresh** button to view updated logical settings and statistics.*

The WAN Logical View displays the following information:

IF
Displays the interface index; a unique value for each interface that this device connects to.

Protocol
Displays the active Link Layer protocol. This field displays PPP (Point to Point), Frame Relay, or Other.

Compression
Indicates whether data compression is activated or de-activated.

NOTE

Data compression is not supported by the DELHW-UA at this time; therefore, compression will always be de-activated or "Off".

MTU
Displays the MTU (Maximum Transfer Unit) for this interface. The MTU is the largest packet size that can be transmitted on the selected interface.

Line Coding
Displays the line coding set for this interface. The field displays INV-HDLC, JBZS, or None. None (the default value) is displayed when the line coding being used on the interface is B8ZS.

CRC Length
The length of the CRC (Cyclical Redundancy Check) for this interface.

Changing WAN Logical Settings

To change the protocol setting from your WAN Logical View window:

1. In the WAN Logical View window's list, click on the interface of interest, and the WAN Logical Settings window (Figure 7-2) will appear.

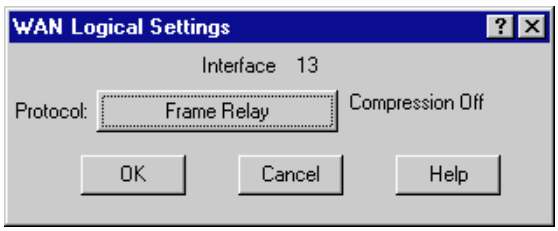


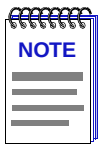
Figure 7-2. The WAN Logical Settings Window

2. Use the **Protocol:** field to select **PPP**, **Frame Relay**, or **None**. **LEX** (LAN Extender) may also appear in the Protocol menu, but it is not applicable to a DELHW-UA device.

3. After making your changes, click on **OK** to exit the window and save the changes, or **Cancel** to exit the window without saving the changes.

Note that this window also displays the state of compression on the interface.

After exiting the Logical Settings window, the WAN Logical View window will update to display the changes you made.



If you do make any configuration changes through the WAN Logical Settings window, make sure they don't conflict with other configurations made through the QuickSET for the DELHW-UA application.

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W